Türk Sosyal Bilimler Araştırmaları Dergisi /Journal of Turkish Social Sciences Research
Nisan 2023 Cilt: 8 Sayı: 1
Hasan Kalyoncu Üniversitesi
Gaziantep

TERÖRİZMİN FİNANSMANI VE KRİPTO PARALAR

Prof. Dr. Taner AKÇACI
akcaci@gantep.edu.tr
ORCID: 0000-0002-5343-0894

Dr. Öğr. Üyesi Ali GÖK
aligok86@gmail.com
ORCID: 0000-0002-0734-459X

ÖZ: Teknolojinin ilerlemesiyle birlikte internet üzerinden daha kolay, hızlı ve ucuz küresel transferler sağlayan kripto paralar, kullanımlarının yaygınlaşması ile birlikte aynı zamanda terör örgütlerinin eylemlerini destekleyen yeni dijital gelişmelerden biri olma olasılığı taşımaktadır. Çalışma, kripto paraların, takibin ve kontrolün zor olduğu internet üzerinden terör örgütleri açısından finansman yaratma ve değer aktarma avantajına sahip olduğunu iddia etmekle birlikte, terör örgütlerinin kripto paraları kullanma arayışında olmalarının altında yatan nedenleri incelemeyi amaçlamıştır. Çalışmada öncelikle terör örgütlerinin neden finansmana ihtiyaç duydukları ve bu ihtiyaçları karşılamak adına hangi finansman kaynaklarını kullandıkları ortaya konulmuş, akabinde internetin terör örgütlerine finansman kaynakları yaratmak ve bu kaynakları yönetmek açısından ne gibi avantajlar sağladığı ele alınmıştır. Son olarak ise kripto paraların genel özellikleri ve terör örgütlerinin söz konusu özelliklerden neden yararlanmaya çalıştıkları örnekler üzerinden tartışılmıştır.
Anahtar Kelimeler: Terörizm, terörizmin finansmanı, kripto paralar, karanlık ağ, derin ağ.

FINANCING OF TERRORISM AND CRYPTOCURRENCY

ABSTRACT: With the advancement of technology, cryptocurrencies, which provide easier, faster and cheaper global transfers over the internet, have become widespread in use and because of that it is likely to be one of the new digital developments that support the actions of terrorist organizations. The study claims that cryptocurrencies have the advantage of creating financing and transferring value for terrorist organizations over the internet, where tracking and control are difficult and study going to aim to examine the underlying reasons why terrorist organizations seek to use cryptocurrencies. In this study, it was revealed the reason of terrorist organizations need financing and which financing sources they use to meet these needs, subsequently, it was discussed what advantages the internet provides to terrorist organizations in terms of creating and managing sources of financing. Finally, the general characteristics of cryptocurrencies and the examples of why terrorist organizations are trying to take advantage of these characteristics have been discussed.

Keywords: Terrorism, financing of terrorism, cryptocurrency, dark web, deep web.

Makale Gönderim Tarihi: 21.12.2022 Makale Kabul Tarihi: 13.04.2023

Citation Information / Kaynakça Bilgisi: Akçacı, T. ve Gök, A. (2023). Terörizmin finansmanı ve kripto paralar, *Türk Sosyal Bilimler Araştırmaları Dergisi*, 8(1), 32-46.

1. GİRİŞ

Terör örgütleri silah/mühimmat gibi teknik ihtiyaçlarını karşılayabilmek, eylemlerini gerçekleştirebilmek, diğer operasyonel faaliyetlerini yürütebilmek, organizasyonlarının işleyişini sürdürebilmek ve ideolojik etki alanına sahip olabilmek için finansman kaynaklarına ihtiyaç duymaktadırlar. Bu doğrultuda da yasal veya yasadışı yöntemlerle işleyen çeşitli finansman kaynakları bulunmaktadır. Terör örgütlerinin finansman kaynaklarının büyük çoğunluğu uyuşturucu, silah ve insan kaçakçılığı gibi yasa dışı gelirler üzerine kurulu olsa da küresel erişime sahip terör örgütleri yasal yöntemlerle ya da hayır kurumları vasıtasıyla bağışlar üzerinden finansman sağlayabilmektedirler.

Yasa dışı gelirler, terör örgütlerinin temel dayanak noktaları olmaya devam ederken, terörizmle mücadelede asıl önemli husus yasal yöntemler üzerine kurulu olması sebebiyle tespiti zor olan finansman kaynaklarının durdurulabilmesidir. Terörizmle mücadele eden kolluk kuvvetleri bu durumun farkında olarak sıkı mali tedbirler alma ve kontrol sağlama eğilimindedirler. Özellikle 11 Eylül saldırıları sonrası finansal kurumlara ve bankacılık sektörüne yönelik düzenlemeler nedeniyle şüpheli aktarımlar tespit edilebilmekte ve yasal kanallar vasıtasıyla finanse edilen bir terör eyleminin gerçekleşme ihtimali zayıflamaktadır.

Ancak terör örgütleri de özellikle internetin yaygınlaşmasının sağladığı avantajlardan faydalanarak alternatif yöntemler geliştirme arayışındadır. Terör örgütleri hem faaliyetlerini desteklemek için gerekli fonları toplamak hem de para transfer etmek için interneti kapsamlı bir şekilde kullanma eğilimindedirler. İnternetin bu bağlamda terör örgütleri için avantajı belirli bir oranda anonimlik ve güvenlik sağlayabilmesidir.

Son dönemlerde ise internet üzerinden daha kolay, hızlı ve ucuz küresel transferler sağlayan kripto paralar gibi yeni dijital araçlar ortaya çıkmıştır. Bu noktada çalışmanın konusunu da oluşturan kripto paraların, terör örgütlerinin eylemlerini destekleyen dijital gelişmelerden biri olma olasılığı bulunmaktadır. Kripto paraların geleneksel para birimine göre çeşitli avantajları ve terör örgütlerinin bu para birimlerinden neden ve nasıl faydalanabilecekleri konusu literatürde tartışmalara yol açmıştır. Ancak bu konuda güvenlik odaklı çalışma ve bilimsel değerlendirme sınırlı sayıda bulunmaktadır. Bu çalışma, söz konusu eksikliği giderebilmek adına terör örgütlerinin kripto paraları kullanma arayışında olmalarının altında yatan nedenleri incelemeyi amaçlamaktadır.

Bu amaç doğrultusunda çalışmada öncelikle terör örgütlerinin neden finansmana ihtiyaç duydukları ve bu ihtiyaçları karşılamak adına hangi finansman kaynaklarını kullandıkları ortaya konacak, akabinde internetin terör örgütlerine finansman kaynakları yaratmak ve bu kaynakları yönetmek açısından ne gibi avantajlar sağladığı ele alınacaktır. Son olarak ise öncelikle kripto paraların genel özelliklerine yer verilecek olup, akabinde terör örgütlerinin söz konusu özelliklerden neden yararlanmaya çalıştıkları örnekler üzerinden tartışılacaktır.

2. TERÖRİZMİN FİNANSMAN KAYNAKLARI

IMF'ye (2022) göre terörizmin finansmanı, *terör amaçlı fonların toplanması veya sağlanması* olarak ifade edilmektedir. Ayrıca, gizlilik ve yasa dışı girişimleri içeren bir *yeraltı* evrenidir ve aynı zamanda küresel finansal sistemine entegre bir yönetim anlayışını içermektedir (Raphaeli, 2003). Raphaeli (2003), terörizmin finansman kaynaklarını geniş topraklara yayılan ve çok çeşitli dini, sosyal, ekonomik ve politik dokunaçları olan bir *ahtapot* olarak tanımlamaktadır. Bu doğrultuda terör örgütlerinin söz konusu dokunaçlar çerçevesinde şekillenen geleneksel olarak beş ana finansman kaynağı bulunmaktadır. Bunlar: meşru yatırımlar, devlet sponsorluğu, bağışlar, hayır kurumları ve gasp, uyuşturucu, silah ve insan kaçakçılığı gibi çeşitli suç gelirleridir (Windle, 2018; Schwarz, Manheim ve Johnston, 2019; Jacobson, 2010; Keatinge, Carlisle ve Keen, 2018; Biswas ve Sana, 2019). INTERPOL'e (2022) göre terörizmin finansmanı ise, "düşük seviyeli dolandırıcılığı, fidye için adam kaçırmayı, kâr amacı gütmeyen kuruluşların kötüye kullanımını, petrol, kömür, elmas, altın ve uyuşturucunun yasa dışı ticaretini ve dijital paraların kullanımını" içermektedir.

Birleşmiş Milletlerin, Terörizmin Finansmanının Önlenmesine İlişkin Uluslararası Sözleşmesi, terörizmin fonlarını, "maddi veya manevi, taşınır veya taşınmaz olarak elde edinilen, her türlü varlık ve elektronik veya dijital de dâhil olmak üzere herhangi bir biçimdeki yasal belge veya araçlar" olarak tanımlamaktadır. Banka kredileri, seyahat çekleri, havaleler, hisse senetleri, menkul kıymetler, tahviller, poliçeler, akreditifler ve bu tür varlıklara veya bunlarla ilgili menfaatler bu tür kaynaklara dâhildir (The

United Nations, 1999). Söz konusu tanımdan da anlaşılacağı gibi terör örgütlerinin *meşru* görünen kaynakları, terörizmin fonları ve yasal fonlar arasında ayrım yapmayı zorlaştırmaktadır. Bu durum kolluk kuvvetlerinin terör örgütlerinin finansman kaynaklarını kolayca tespit edebilmesini de engellemektedir.

Esasen terörün finansman kaynaklarını ve kullanımlarını gizlemek için kullanılan teknikler, kara para aklamak için kullanılanlarla benzer olduğu düşünülmektedir (Schott, 2006). Her iki durumda da aktör finans sektörünü gayrimeşru bir şekilde kullanmaktadır. Bununla birlikte, terörün finansmanı ile ilgili mali işlemler, tespiti engelleyebilmek adına genellikle kara para aklamada olduğundan daha küçük miktarlarda olma eğilimindedir. Ayrıca kara para aklama durumunda, fonlar her zaman yasadışı kaynaklıdır, oysa terörün finansmanı durumunda fonlar hem yasal hem de yasadışı kaynaklardan gelebilmektedir. Bu nedenle, terörizmin finansmanına dâhil olan kişi veya kuruluşların birincil amacı, sadece paranın kaynaklarını gizlemek değil hem finansman faaliyetini hem de finanse edilen faaliyetin doğasını gizlemektir (IMF, 2022). Eğer faaliyet gizlenebilirse, kaynak gelecekteki terör eylemleri için de kullanılabilir durumda kalacaktır (Schott, 2006).

Terör örgütleri çeşitli finansman kaynaklarını değerlendirirken neye göre karar verirler? Bir kaynağı diğerlerinden daha çekici yapan nedir? Genel olarak, terör örgütleri şu altı kritere göre finansman kaynaklarını seçmektedirler: *nicelik, meşruiyet, güvenlik, güvenilirlik, kontrol ve basitlik*. İlk olarak bir terör örgütü, daha etkin faaliyet göstermek ve faaliyetlerini farklı sınırlar arasında genişletmek için daha fazla paraya ihtiyaç duymaktadır. İkinci olarak, terör örgütlerinin kendilerini idame ettirebilmeleri için meşruiyete ihtiyaçları vardır. Belirli finansman kaynakları da bir grubun meşruiyetini çeşitli şekillerde etkileyebilir ve diaspora desteği gibi meşruiyetin bir göstergesi olabilirler. Üçüncü olarak, devletin ve kolluk kuvvetlerinin radarından uzak duracak belirli finansman kaynakları kullanmayı isteyeceklerdir. Dördüncü olarak, terör örgütleri için öngörülebilir ve tutarlı finansman kaynakları, tutarsız bir şekilde dalgalananlardan daha iyidir. Beşinci olarak para genellikle etki ve güçle ilişkilendirilir. Farklı finansman kaynakları, bir terör örgütünü, üyeleri ve operasyonları üzerindeki kontrolünü tehdit edebilir veya güçlendirebilir. Altıncı olarak, kaynak edinme süreçlerinin daha basit ve daha az maliyetli olmasını isterler (Freeman, 2011).

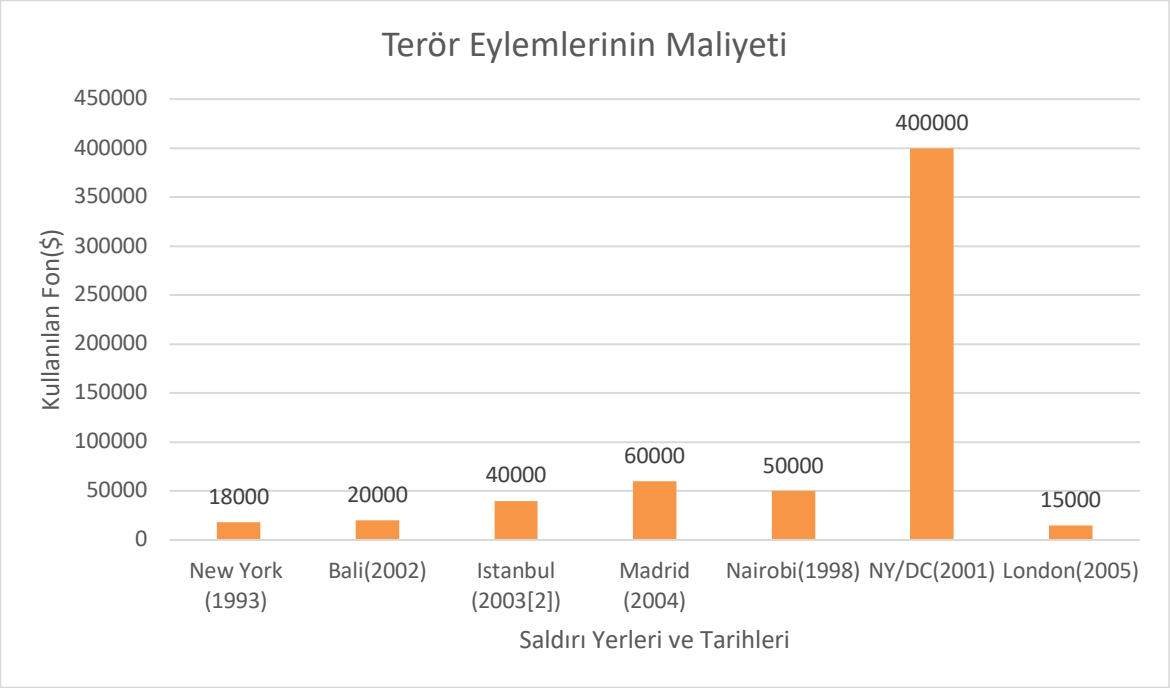
Thachuk ve Lal (2018), terör örgütlerinin son birkaç on yılda istikrarlı bir şekilde *gangsterleştiklerini* düşünmektedir. Özellikle de çok para kazanma konusundaki istekleri, yasadışı uyuşturucu ticaretine dâhil olmalarının birincil nedenidir (Wardhana ve Nugroho, 2021). Çoğu terör örgütü eylemlerinin finansmanını sağlamak için genellikle organize suç örgütlerinin alanı olarak kabul edilen ve onlarla aynı suç taktiklerini kullanabileceği yasadışı ticarete yönelmiştir. Ancak, onları geleneksel organize suç örgütlerinden ayıran temel fark, yasadışı fon toplama motivasyonları (siyasal saik) ve paranın korku atmosferi yaratabilecek geniş çaplı terör eylemleri için harcanma şeklidir (Thachuk ve Lal, 2018).

Bu noktada terör örgütlerinin, terörizmin doğası gereği finansman kaynaklarının büyük çoğunluğu suç üzerine kurulu olsa da küresel çapta organize olmuş terör örgütleri meşru yatırımlara müdahil olarak ya da hayır kurumlarına etki ederek bağışlar üzerinden gelir sağlayabilmektedirler (Conway, 2006; Schott, 2006). Özellikle hayır kurumları veya insani yardım kuruluşları istismara açık olmaları ve sempatizanların *insani yardım* gibi hassas noktalarına dokunulmasını sağladıkları için, terör örgütleri tarafından yoğun bir şekilde kullanılmaktadırlar. Bazı hayır kurumları açıkça terörü finanse etmek amacıyla kurulurken, bazıları da içlerine sızılarak kullanılmaktadır (Jacobson, 2010). Wilkinson (2005), özellikle destekçilerinden veya sempatizanlarından alınan bağışların/gelirlerin terör örgütlerinin eylemlerini sürdürmek için daha fazla finansman, silah ve asker elde etmelerine yardımcı olduğunu ifade etmektedir.

Örneğin El Kaide ve DEAŞ gibi terör örgütleri daha geniş coğrafyada etki alanına sahip olma iddiasında oldukları için sempatizanlarından bağış toplayabilecek/gelir elde edebilecek sisteme sahiptir (Schwarz, Manheim ve Johnston, 2019). Bu çerçevede DEAŞ terör örgütü, küresel bağışların yanı sıra, Irak ve Suriye'de toprak kontrolü sağlayarak (özellikle Rakka ve Musul gibi kilit şehirler de dâhil olmak üzere) hem vergilendirme hem de haraç yoluyla nüfustan gelir elde edebilmiştir. Aynı zamanda yerel ekonomi üzerinde kontrol sağlayarak da bunu bir finansal kaynak zenginliğine dönüştürmüştür (Clarke ve Williams, 2018). Ancak öbür yandan bu etki alanına sahip olabilmek adına da daha fazla kaynak yaratmak ve bu kaynakları geniş coğrafyadaki elemanlarına aktarabilmek durumunda kalmıştır. Bu nedenle de birçok ülkede özellikle bağış toplayabilmek adına çeşitli finansal ağlara sahip olarak faaliyetlerini yürütebilme arayışındadır (Schwarz, Manheim ve Johnston, 2019). Bu doğrultuda tüm terör örgütleri için paranın

hareketinin kritik bir aracı adım olduğunu söylemek mümkündür. Çünkü terör örgütleri çoğunlukla bulundukları yerden veya eylemlerini gerçekleştirebilecekleri yerlerden farklı yerlerde para toplarlar. Terör örgütlerinin eylemlerini gerçekleştirebilmek için parayı, kaynaklarından ihtiyaç duyulan operasyonel alanlara taşıyabilmeleri gerekir (Freeman ve Ruehsen, 2013). Bununla birlikte, saldırılar arasında işe alım, planlama ve tedarik sağlamak için bir terörist ağının veya belirli bir hücrenin sürdürülmesi de finansal kaynaklara ihtiyacı temsil eder (Financial Action Task Force, 2008).

O halde terör örgütü için paranın hareketi bir eylemin gerçekleştirilmesinde çok önemlidir. Aşağıdaki şekilde 1993-2005 yılları arasındaki geniş çaplı terör eylemlerinin ortalama maliyetlerini ortaya koymaktadır. Şekilde 11 Eylül saldırılarında görüldüğü gibi eylemin boyutu arttıkça maliyet yükselmekte ve maliyetle doğru orantılı olacak şekilde finansman kaynaklarına ihtiyaç da artmaktadır.



Şekil.1. Terör Eylemlerinin Maliyet Analizi

Kaynak: Biersteker ve Eckert (2008).

Bu noktada cevaplanması gereken önemli soru, terör örgütlerinin eylemlerini finanse edebilmek adına parayı nasıl aktardıklarıdır. Terör örgütleri, finans sektörü, nakit paranın kuryeler tarafından fiziksel hareketi ve ticaret sistemi yoluyla malların hareketi de dâhil olmak üzere, kuruluşlar içinde ve arasında para taşımak için çok çeşitli yöntemler kullanırlar (Financial Action Task Force, 2008). Freeman ve Ruehsen'e (2013) göre yaygın olarak kullanılan altı yöntem bulunmaktadır. Bunlar: *nakit kuryeler, gayri resmî transfer sistemleri (örneğin hawala*[1]*), para hizmeti işletmeleri, resmî bankacılık, sahte ticari faturalandırma ve yüksek değerli malların temini*.

Para aktarımına dâhil edilen küçük miktarlar, genellikle terör örgütünün ya da alıcının tespit edilmesini neredeyse imkânsız hale getirmektedir (Normark ve Ranstorp, 2015). Ancak miktar artıkça risk de artmaktadır. Bu nedenle terör örgütleri parayı aktarırken, hacim, risk, kolaylık, maliyetler ve hız

[1] Hawala, resmî bankacılık sistemine alternatif olarak (genellikle ondan bağımsız olarak) çalışan gayri resmî bir fon transfer sistemidir. Bu tür sistemler başlangıçta, uzak bölgeler arasında belirli bir zamanda veya geleneksel bankacılık araçlarının bulunmadığı, zayıf veya güvensiz olduğu bölgelerde ticareti kolaylaştırmak için geliştirilmiş, ancak zamanla yasadışı faaliyetlerde kullanılmaya başlanmıştır (Chêne, 2008). Kişisel güvene dayalı olduğu belirtilen bu sistemde para transferi yapmak isteyen kişi, bulunduğu yerdeki bir operatörle iletişime geçmekte ve transfer etmek istediği para için bir komisyon ödemektedir. Parayı alacak kişi ise, başka bir yerde, yerel operatörle iletişime geçmekte ve parayı komisyon düşülerek tahsil etmektedir (Jost ve Sandhu, 2013).

konularını dikkate alarak uygun yöntemleri seçmektedirler. Örneğin resmî bankacılık, havale ve para transferi işletmelerinin kullanımı gibi yöntemler teorik olarak tek bir işlemde yüksek miktarda para transferine olanak sağlayabilir. Buna karşılık, transfer edilen paranın boyutu düşünüldüğünde en belirgin riskler arasında transferin yetkililer tarafından tespit edilmesi yer almaktadır. Örneğin, iki banka arasındaki bir havalenin izlenmesi, kaydedilmesi ve keşfedilmesi, Afganistan ve Pakistan arasındaki sınırı geçen bir nakit transferinden çok daha olasıdır (Freeman ve Ruehsen, 2013).

Bir diğer husus ise, para henüz terör örgütünün doğrudan kontrolü altında değilse veya operasyonel güvenlik endişeleri nedeniyle aktarılamıyorsa diğer transfer mekanizmalarının kullanılmasıdır. Bu durum özellikle küresel piyasalara erişim ihtiyacı hisseden DEAŞ gibi terör örgütleri için daha kritiktir. Örneğin daha çok devlet sponsorluğuna dayanan Hizbullah terör örgütünün İran bankacılık sistemine erişimi varken, El Kaide veya DEAŞ gibi terör örgütlerinin genellikle başka yöntemler kullanması gerekmektedir (Schwarz, Manheim ve Johnston, 2019).

Özellikle 21. Yüzyılda teknolojinin getirdiği yenilikler ve internetin yaygınlaşmasıyla birlikte *dijital* ekonominin gelişimi terör örgütlerinin hem kaynak yaratmada hem para aktarmada hem de parayı yönetmek adına farklı yöntemleri keşfetmelerine olanak sağlamıştır (Goldman, vd, 2017). Carroll ve Windle'ye (2018) göre bu bakımdan, birçok geleneksel yöntem de siber kullanım yoluyla etkinleştirilebilir ve geliştirilebilir hale gelmiştir.

Bir sonraki bölümde internetin terör örgütlerine finansman kaynakları yaratmak ve bu kaynakları yönetmek açısından ne gibi avantajlar sağladığı ele alınacaktır.

3. İNTERNETİN TERÖRİZMİN FİNANSMAN KAYNAKLARINA ETKİSİ

İnternet ticaret için uygun fiyatlı, anonim, güvenli, coğrafi olarak sınırsız ve büyük ölçüde düzenlenmemiş bir ortam olarak, kullanıcılara finansal işlemleri yürütmek ve fikir alışverişinde bulunmak için benzeri görülmemiş bir küresel pazar ağı sağlamaktadır. Ancak aynı zamanda bu özellikler interneti, geniş dolandırıcılık planları, kara para aklama ve suç ortakları arasındaki iletişim için de davetkâr bir ortam haline getirmektedir (Hinnen, 2004). Terör örgütleri de stratejik hedeflerini ilerletmek için internetin taktiksel olarak kullanabilecekleri güçlü bir araç olduğunun farkındadır (Aly, Macdonald, Jarvis ve Chen, 2017). Bu çerçevede internet altyapısını, finansman kaynakları oluşturmak, para aktarmak ve paralarını yönetmek için kullanabilme eğilimindedirler (Conway, 2006). Hinnen'e göre terör örgütleri interneti finansman maksatlı dört şekilde kullanmaktadır. Bunlar:

1- Doğrudan bağış talepleri: Web siteleri, sohbet grupları ve hedefli elektronik postalar aracılığıyla taraftarlarını ikna ederek doğrudan bağışlar talep etmektedirler.

2- Hayır kurumlarının paravan olarak kullanılması: Bir kesimi giydirmek, beslemek ve eğitmek gibi açık bir amaçla, ancak bağışta bulunanların cömertliğini şiddet eylemlerini finanse etmek için kullanmak gibi gizli bir niyetle para toplayarak hayır kurumlarından yararlanmaktadırlar.

3- Siber (çevrimiçi) suçlar: Kimlik ve kredi kartı bilgilerinin hırsızlığı, fikri mülkiyet korsanlığı ve dolandırıcılık gibi çevrimiçi suçları işlemektedirler ve bu suçların gelirleriyle misyonlarını desteklemektedirler.

4- İletişim: Fon yaratma faaliyetlerini organize etmek ve uygulamak için interneti yaygın ve anonim bir iletişim aracı olarak kullanmaktadırlar (Hinnen, 2004).

Bu yöntemler geleneksel coğrafi engelleri kaldırma noktasında teknolojinin terör örgütlerine sağladığı avantajların başında gelen özellikle *derin ağ* (deep web) ve *karanlık ağ* (dark web) ile bunlara erişim imkânı sağlayan *Tor, I2P ve FreeNet* gibi platformlar üzerinden kullanılmaktadır (Keatinge, Carlisle ve Keen, 2018).

Tablo 1. İnternetin Katmanları

İnternetin 3 Katmanı	Erişim Yolu	Erişim Kısıtlaması	Yasallık Durumu
Yüzey İnternet	Yahoo!-Google-Reddit-Bing-Facebook-Twitter-Instagram	Erişim kısıtlaması bulunmamakta	Yasal
Derin Ağ	TOR-12P-FreeNet	Erişim yalnızca TOR-12P-FreeNet üzerinden	Birçok ülkede yasal (ABD, İngiltere, Hollanda)
Karanlık Ağ	TOR-12P-FreeNet	Erişim yalnızca TOR-12P-FreeNet üzerinden	Yasal Değil

Kaynak: Sönmez ve Çelik (2020).

Tablo 1'de görüldüğü gibi internetin görünen yani yüzey kısımda Internet Explorer ya da Chrome vs. gibi tarayıcılar üzerinden web sayfalarına ya da sosyal medya platformlarına erişim sağlanabilirken, internetin gizli kısmı olarak görülen derin ağ ve onun karanlık yüzü olarak adlandırılan karanlık ağa ise söz konusu tarayıcılarla erişim sağlanamamaktadır. Derin ve karanlık ağa Tor (The Onion Router), I2P (Invisible Internet Project/Görünmez İnternet Projesi) ve FreeNet gibi yazılımsal özel platformlar ile erişim sağlanabilmektedir (Sönmez ve Çelik, 2020; Başaranel, 2021).

Kullanıcılar karanlık ağa erişim halindeyken, Tor yazılımına entegre olmuş *güvenli e-posta, web sohbetleri veya kişisel mesajlaşma vb.* yöntemlerle ve bir dizi sanal tünel aracılığıyla çevrim içi katman ağlara bağlanabilmekte ve birbirleriyle iletişim sağlayabilmektedirler. Bu sayede kullanıcılar, kimliklerini gizli tutarak, halka açık ağlar üzerinden bilgi paylaşabilmektedirler (Türkşen, 2021a).

Terör örgütleri de özellikle karanlık ağı, çalıntı kredi kartı bilgilerini elde etmek veya uyuşturucu satışı yapmak için kullanmaktadır. Bunun dışında pasaportlar ve sahte belgeler temin etmek, silah ve mühimmat satın almak da karanlık ağın terör örgütleri tarafından kullanılma amaçları arasındadır (Keatinge, Carlisle ve Keen, 2018).

Paoli'ye (2017) göre yüzey interneti üzerinden mal ve hizmet satın almak ile karanlık ağ pazarlarında işlemlerin gerçekleşme şekilleri arasında belirli benzerlikler bulunmaktadır. Paoli (2017), alıcılar, satın almak istedikleri ürünü belirledikten sonra, ürün listeleme sayfasında yüzey internetinde olduğu gibi *şimdi satın al* bölümüne tıklayarak ve alıcıların ilgili sisteme kaydolarak satın alma işleminin gerçekleştirildiğini, aradaki en önemli farkın ise ödeme şekli olduğunu ifade etmektedir.

Bu alanlarda söz konusu faaliyetlerin gerçekleştirilmesine PayPal gibi araçlar da olanak sağlarken, günümüzde kripto paralar da kullanılarak daha fazla anonimlik sağlanması hedeflenmektedir. Kripto paralar hem Tor gibi yazılımlarla birlikte kullanılarak karanlık ağda hem de kendi sahip olduğu veri tabanı içerisinde özellikle terör örgütlerinin alternatif finansman kanalını oluşturmaya başlamıştır.

3.1. Kripto Paralar ve Terörizmin Finansmanı

Kolluk kuvvetlerinin terörizmin finansmanıyla mücadelede temel yöntemi fon transferlerini takip etmektir. Bu nedenle bankalar üzerinden gerçekleştirilen işlemler yakından takip edilmektedir. Terör örgütleri de finansman kaynaklarının tespit edilmesini ve bu kaynakların kesilmesini engelleyebilmek adına banka dışı fon transferleri gibi takip edilmesi zor yöntemler arayışındadır.

Özellikle yasal işletmelerin kullanılması, yetkililere terör ağı veya örgütü hakkında daha fazla bilgi verebilmektedir. Yasal bir iş, yetkililere terör örgütüne bir kapı sunan bir işaret feneri işlevi görebilmekte ve örgütün finansal işleyiş tarafına doğru iletişimi veya para akışını takip etmelerine izin verebilmektedir (Freeman, 2011).

Kripto paralar kullanılarak yapılan işlemler, alıcıların ve satıcıların gerçek kimlikleriyle mutlaka bağlantılı değildir. Bu durum, yasa dışı işlemlerin izlenmesini zorlaştırmaktadır (Paoli, 2017). Bu nedenle yöntem arayışı çerçevesinde kripto paraların ortaya çıkması ve yaygınlaşması terör örgütlerinin de dikkatini çekmiştir.

Kripto paralar üzerinde tanımsal bir belirsizlik bulunmakla birlikte, bazıları onları bir meta ya da meşru bir ödeme şekli olarak görmekte, bazıları ise gizli bir ödeme yöntemi, mutlak bir hak ve mülkiyet kaydı veya ödül puanlarına çok benzeyen bir teşvik mekanizması olarak değerlendirmektedir. Bu tanımsal belirsizlik hukuksal düzenlemeleri zorlaştırmakla birlikte, terör örgütlerinin finansman kaynakları için boşluklardan yararlanmalarını sağlamıştır (Kfir, 2020). Bu bölümde öncelikle kripto paraların genel özelliklerine yer verilecek olup, akabinde terör örgütlerinin söz konusu özelliklerden neden yararlanmaya çalıştıkları tartışılacaktır.

3.1.1. Kripto Paraların Genel Özellikleri

Son on yılda, daha kolay, hızlı ve ucuz küresel ödemeler ve transferler vaat eden yeni dijital araçların sayısında olağanüstü bir artış görülmüştür (Schwarz, vd., 2021). Söz konusu dijital araçların arkasındaki teknoloji sürekli geliştikçe ödeme sistemleri de değişmektedir (Kfir, 2020). Bugün piyasada birçoğu mobil erişim, internet ve dijital depolama alanı gibi platformlar üzerine kurulmuş çeşitli yenilikçi ödeme sistemleri bulunmaktadır. Bu alternatif ödeme sistemlerine örnek olarak *PayPal, Apple Pay, Google Cüzdan, Alipay, Tenpay, Venmo, M-Pesa, BitPay, Moven, BitPesa, PayLah, Dash, FAST, Transferwise vb.* verilebilir. Geleneksel para birimine dayalı ödeme sistemlerinin ötesinde, özellikle dijital paraların artan kullanımı, mal ve hizmetlerin finansmanında da daha hızlı, daha esnek ve daha yenilikçi ödemeler ve yollar sağlamıştır. Bu noktada dijital paralarda, internetin gücünü kullanan başta Bitcoin olmak üzere kripto paralar öne çıkmaktadır (Nian ve Chuen, 2015).

Kavramsal açıdan değerlendirildiğinde, *crypto ve currency* kelimelerinin bir araya gelmesiyle ortaya çıkan *cryptocurrency*, kripto (şifreli) para anlamına gelmekte ve "internet aracılığıyla kullanılan, hiçbir merkezi otoriteye ya da aracı kuruma bağlı olmayan, sanal para birimini" ifade etmektedir (Eğilmez, 2017). Söz konusu paralardan ilk olarak 2009 yılında Bitcoin piyasaya sürülmüş ve o zamandan beri değişen derecelerde binlerce kripto para oluşturulmuştur (Schwarz, vd., 2021). Günümüzde *Ethereum, XRP, EOS, Litecoin vb.* gibi kodlarında ve kodlanma şekillerinde kriptografinin kullanıldığı para birimlerine verilen çeşitli isimlerde kripto paralar mevcuttur (İşler, Takaoğlu ve Küçükali, 2019). Bu paralar fiat para birimlerinden farklı özelliklere sahip olmakla birlikte, aşağıda Tablo 2'de söz konusu farklar belirtilmiştir.

Tablo 2. Fiat Para Birimi ile Dijital Para Birimi Arasındaki Farklar

Güncel Tipoloji	**Fiat (İtibari) Para Birimi**	**Dijital**
Nedir?	-Egemen -Merkezileşmiş -Anonimlik değişiklik gösterir (nakit anonimliğinden finans kurumları içinde işlem yapan müşterilerin takibine kadar) -Küresel erişim vardır, ancak belirli ülkelerde kullanılmak üzere dönüştürülmesi gerekebilmektedir -İşlemler nakit olarak anlık yapılabilir veya finansal kurumlar aracılığıyla günler sürebilir	-Egemen değildir -Merkezi olanı da olmayanı da vardır -Anonimlik değişiklik gösterir (takma ad ya da anonim) -Küresel erişim vardır ancak itibari para birimi kadar yaygın olarak kullanılmamakta ve kabul görmemektedir -İşlemler saniyeler içerisinde gerçekleştirilebilir
Neye benzer?	-Nakit Para ($, €)	-E-gold, Liberty Reserve, Linden Dollars, Bitcoin
Nasıl kullanılır?	- İnsandan insana (elden ele) -Elektronik olarak aracı şirketler vasıtasıyla (Paypal, Visa-Mastercard)	-İnsandan insana (sanal) -Elektronik olarak (Bitcoin alışverişi)

Kaynak: Goldman, vd. (2017).

Eğilmez'e (2017) göre, kripto paraların fiat para birimlerinden en önemli farkı, bu paraların herhangi bir devletin merkez bankasına bağlı olmaması sebebiyle, hiçbir devletin ekonomik unsurlarından etkilenmemesidir.

Kripto paralar, geliştiricileri tarafından dağıtılan dijital paraların bir alt kümesidir. Bununla birlikte birçok dijital paradan farklı olarak, kripto paralar yalnızca geliştiricisinin güvenilirliği ve kontrolü ile değil, esas olarak işlem biriminin teknolojik temeli ile desteklenmektedir (Whyte, 2019). En iyi bilinen dijital varlıkların bazıları, işlemleri güvence altına almak ve blok zinciri gibi dağıtılmış defter teknolojisi (DLT) tarafından desteklenen ek birimlerin oluşturulmasını kontrol etmek için kriptografik teknolojiye güvenmektedir (Schwarz, vd., 2021).

İşlemleri doğrulama eylemi yoluyla defter sistemine katkıda bulunma süreci rekabetçi ve pahalıdır. Ancak geliştiriciler (ki bu herkes olabilir) sürekli olarak para hacmi ile aşamalı olarak ödüllendirilmektedir. Böylece bir bütün olarak sistemin güvenliğine yatırım teşvik edilmekte ve mevcut paraların nihai hacmi kontrol edilebilmektedir (Whyte, 2019).

Kripto paralar, işlemleri doğrulamak için kriptografik kanıtlara dayanan ve bir banka veya finans kurumu gibi bir üçüncü tarafa güvenmeden ağ etkinliği hakkında fikir birliği sağlayan açık kaynaklı P2P değer aktarım ağlarına sahiptir. Kripto paralar P2P'yi, iki taraf arasında doğrudan transferleri etkinleştirerek, bir *dijital aktarım* aracı olarak kullanmaktadır. Bu anlamda alan ve mesafe sınırlamaları olmadan tıpkı iki kişinin fiziksel fiat para birimini değiştirebilmesine benzemektedir (Keatinge, Carlisle ve Keen, 2018). Bu sistemin en önemli özelliği ise, "tek bir noktada tutulmak yerine, birden fazla yerde yani bir ağın tamamında tutulmasıdır." Bir ağın tamamında tutulmasının temel sebebi, sisteme alınan bilgilerin güvenilirliğini sağlamaktır. Bu sayede kayıt yerlerinden herhangi birinin kaybolması durumda bilgilerin, ağda bulunan diğer kayıt yerlerinde muhafazası sağlanabilmektedir (Eğilmez, 2017).

Her para birimi, bir işlem kanıtının (proof of work) ardından oluşmaktadır. İşlem kanıtı, kullanıcının bilgisayarının (bir düğümün) karmaşık matematiksel problemleri çözmesini kapsamakla birlikte, buna madencilik (mining) denilmektedir. Madencilik, "sonucu çözülmüş işlemlerin kripto para ağında kalıcı olarak kaydedilen veri kümeleridir, bunlar her para birimine ait işlemlerin bir kaydıdır" (Türkşen, 2021b).

Ağı çalıştırma adımları ise aşağıdaki gibidir:

1- Yeni işlemler tüm düğümlere yayınlanır.

2- Her düğüm yeni işlemleri bir blokta toplar.

3- Her düğüm, kendi bloğu için zor bir iş kanıtı bulmaya çalışır.

4- Bir düğüm bir iş kanıtı bulduğunda, bloğu tüm düğümlere yayınlar.

5- Düğümler, yalnızca içindeki tüm işlemler geçerliyse ve henüz harcanmamışsa bloğu kabul eder.

6- Düğümler, zincirdeki bir sonraki bloğu oluşturmaya çalışarak bloğu kabul ettiklerini ifade eder.

Düğümler her zaman en uzun zincirin doğru olduğunu düşünür ve onu uzatmak için çalışmaya devam eder (Nakamoto, 2018).

Ağlara erişimi sağlayan ise para cüzdanlarıdır. Bir kripto para cüzdanı, özünde bir kullanıcının blok zincirinde görünen genel kripto para adresleriyle ilişkili işlemleri imzalamak için kullanılan parolalar olan kullanıcıların *özel anahtarlarını* temsil eder. Özel anahtarlara sahip olan kişi, ilgili kripto paranın fiili sahibidir (Keatinge, Carlisle ve Keen, 2018).

Çarkacıoğlu'na (2016) göre kripto paralarda üçüncü bir tarafın olmaması nedeniyle güven gereksizdir. Sistemin güvenliği, karşılıklı birbirine güvenmeyen madenciler aracılığıyla ve bu madencilerin büyük defter tutma ve bundan finansal teşvik edinme arzuları olduğu ilkesi temelinde sağlanır (Çarkacıoğlu, 2016).

Bugün kripto para ekosistemi, binden fazla farklı kripto varlık içermektedir. Bu varlıklar, Bitcoin'in kendisinin bariz istisnası dışında, genellikle *altcoin* olarak adlandırılır. Birçok altcoin, uyarlanmış blok zinciri protokollerinin benzersiz uygulamaları nedeniyle Bitcoin'in sunduğundan daha fazla katma değere sahiptir. Örneğin Ripple adlı bir şirket, yalnızca bir kripto paranın değil, aynı zamanda bankaların aynı blok zinciri teknolojisine dayalı para transferlerini güvence altına almaları için bir işlem platformunun geliştirilmesinin arkasında olmuştur. Benzer şekilde ZeroCash gibi diğer altcoinler, işlemleri daha da anonimleştiren ek havuzlama adımlarını içeren yeni protokollere sahiptir (Whyte, 2019).

Kripto paraların bir diğer özelliği de bazılarının dönüştürülebilir bazılarının ise dönüştürülemez olmasıdır. Dönüştürülemeyen paralar kapalı bir dijital platformda çalışır ve fiat para birimine çevirmek için onaylanmış hiçbir mekanizma bulunmamaktadır. Dönüştürülebilir olanlar ise fiat para biriminde tanımlanmış bir eşdeğer değere sahiptir ve değişken veya sabit oranlar aracılığıyla değiştirilebilir. Bazı

kripto paralar ise, nakit alışverişlerinin neredeyse tamamen anonimliği ile geleneksel bankacılık sistemi aracılığıyla çevrimiçi ödemelerin izlenebilirliği ve ifşası arasında yer alırlar ve bu da onları terör örgütleri gibi gizlilik konusunda endişeli kullanıcılar için çekici hale getirir (Goldman, vd, 2017).

Sonuç olarak kripto paralar, takibin ve kontrolün zor olduğu internet üzerinden terör örgütleri açısından finansman yaratma ve değer aktarma avantajına sahiptir. Bir sonraki bölümde terör örgütlerinin kripto paralardan nasıl yararlanmaya çalıştıkları açıklanacaktır.

3.1.2. Kripto Paraların Terör Örgütleri Tarafından Kullanımı

Terör örgütleri, faaliyetlerinde ve finansman kaynaklarında küresel erişime sahiptir. Yasal veya yasadışı yöntemlerle ve genellikle dolambaçlı yollardan işleyen çeşitli finansman kaynakları vardır. Bu nedenle terörizmle etkili bir mücadele için, finansman kaynaklarının ve para akışının kaynağında durdurulması gerektiği açıktır. Bu, sıkı mali prosedürlerin ve kontrollerin yardımcı olabileceği alanlardan biridir (Raphaeli, 2003). Sıkı mali prosedürlerle ve kontrollerle karşılaşan terör örgütleri de kripto paralar gibi alternatif yöntemlere yönelme arayışındadır.

Kripto paraların bir önceki bölümde bahsedilen avantajlı özellikleri, *Bitcoin, Ethereum, LiteCoin, IOTA, Monero vb.* gibi paraların belli dönemlerdeki değer artışlarıyla birleştiğinde, terör örgütlerinin bu yeni finansal alandan nasıl yararlanabilecekleri konusunda endişelere yol açmıştır (Whyte, 2019). Özellikle 2009 yılında piyasaya sürüldüğünden beri kullanımı artan Bitcoin, devletlerin kolluk kuvvetlerinde endişeye neden olmuştur. Bu durumun temel sebebi Bitcoin'in anonim bir doğasının olması, geleneksel finans alanlarının tersine eşler arası bir platform olarak tasarlanması ve son olarak da işlemlerin küresel olması sebebiyle, geri döndürülemez olmasıdır. Söz konusu hususlar, Bitcoin dışında yeni kripto paraların da ortaya çıkmasıyla ve hukuksal düzenlemelerdeki zorluklar ve gecikmelerle birlikte değerlendirildiğinde, terör örgütleri finansman kaynakları için kripto paraları kullanma eğiliminde olmuşlardır (Oral ve Yeşilkaya, 2021).

Bitcoin gibi yüksek oranda işlem gören kripto paralar diğer bazı kripto paralara göre daha izlenebilir ve daha güvenli olsa da yasadışı faaliyetler giderek daha az bilinen, daha gizli ve özel kripto paralara kaymıştır. Söz konusu kripto paraların blok zinciri daha kısa bir ömre sahip olduğundan takip edilmesi daha da zor olmaktadır. Bu tür kripto paralar özellikle terör örgütlerinin ilgisini çekebilmektedir (Patel ve Pereira, 2021). Genel olarak özellikle anonim olarak tanımlanan kripto paralar, terör örgütlerinin finansman yöntemlerini hem devlet kurumlarından hem de kolluk kuvvetlerinden gizlemeleri için ideal yol olarak görülmektedir (Wolf, 2021).

Tablo 3'te de görüldüğü gibi Schwarz, Manheim ve Johnston'a (2019) göre terör örgütlerinin finansman faaliyetlerinin kripto paralar açısından *daha az, orta ve kritik* olmak üzere üç önem derecesi bulunmaktadır.

Tablo 3. Terör Örgütlerinin Finansman Faaliyetlerinin Kripto Paralar Açısından Önem Derecelerinin Değerlendirilmesi

	Bağış	**Yasadışı Uyuşturucu ve Silah Kaçakçılığı**	**Havale ve Transfer**	**Eylem/Saldırı Finansmanı**	**Operasyonel Finansman**
Anonimlik	Orta önem	Kritik önem	Orta önem	Kritik önem	Daha az önem
Kullanılabilirlik	Kritik önem	Daha az önem	Daha az önem	Daha az önem	Daha az önem
Güvenlik	Orta önem	Kritik önem	Kritik önem	Kritik önem	Kritik önem
Kabul Etme	Daha az önem	Daha az önem	Daha az önem	Orta önem	Orta önem
Güvenilirlik	Daha az önem	Orta önem	Kritik önem	Kritik önem	Orta önem
Hacim	Orta önem	Daha az önem	Kritik önem	Daha az önem	Kritik önem

Kaynak: Schwarz, Manheim, ve Johnston (2019).

Schwarz, Manheim ve Johnston (2019), kripto paraların güvenilirliği ve hacmi gibi tablo 3'te yer alan diğer tüm önemli özellikler birlikte düşünüldüğünde, mevcut hiçbir kripto paranın terör örgütlerinin tüm finansal ihtiyaçlarını tam olarak doğrudan karşılayamayacağını, ancak bununla birlikte, özellikle

iyileştirilmiş kullanılabilirliği olan Bitcoin gibi kripto paraların özellikle bağış toplamada cazip olabileceğini ve terör örgütlerinin kripto paraları bu amaçla kullanabileceğine dair bazı kanıtların ortaya çıktığını düşünmektedirler.

Terör örgütleri tarafından kripto paraların kullanılmasını kolaylaştıran ise *Dark Wallet* ya da *karıştırıcı* (Bitcoin mixer) gibi yazılımlardır. Amir Taaki isimli yazılımcı, 3D baskılı silah yaparak manşetlere çıkan Cody Wilson ile birlikte, Bitcoin kullanan kişilerin kimliğini potansiyel olarak gizleyebileceği Dark Wallet yazılımını geliştirmiştir. Söz konusu yazılımın amacı, Bitcoin ile yapılan işlemlerin takibini neredeyse imkânsız hale getirmektir (Copestake, 2014). Benzer şekilde *Bitcoin Fog* gibi karıştırma hizmetleri de kullanıcıların kripto paraları başka kullanıcılar ile karıştırmasına izin vererek, paraların varış adresini tespit etmeyi neredeyse imkânsız kılmaktadır (Karaman, 2021).

Eryılmaz'ın (2022) ifadesine göre kripto paralar ilk olarak Selefi düşünceye sahip ve Irak direnişinde rol alan *Mücahit Şura Meclisi'nin* organize ettiği bir sosyal medya bağış toplama kampanyasında Bitcoin ile para toplanması ile kullanılmıştır. Günümüzde ise kripto paraların başta DEAŞ olmak üzere birçok terör örgütü tarafından kullanılmaya çalışıldığı ifade edilmektedir (Eryılmaz, 2022).

Irwin ve Milad'ın (2016) ifadesine göre terör örgütleri tarafından Bitcoin ve diğer kripto paraların geniş çapta kullanıldığına dair somut kanıt bulmak zor olsa da bunların Avrupa ve Endonezya'daki bir dizi terör saldırısıyla bağlantılı olduklarına dair güçlü kanıtlar bulunmaktadır. 2021 yılının Haziran ayında Birleşmiş Milletler Terörle Mücadele Haftası kapsamında yapılan toplantılarda da terör örgütlerinin dijital finansmanına odaklanılarak, çevrimiçi kaynaklar aracılığıyla para ve bağış toplama fırsatlarını artırdıkları ifade edilmiştir (Wolf, 2021).

Özellikle DEAŞ, geleneksel fon transferi yöntemleriyle ilişkili bazı riskleri azaltmak için Bitcoin gibi yeni ve gelişmekte olan teknolojilerin kullanımını aktif olarak denemekte ve teşvik etmektedir. Örneğin söz konusu terör örgütüyle bağlantılı bazı siteler kesintisiz ve anonim fon transferine izin verdiği için kripto paralar ile bağış toplamaya çalışmaktadır (Irwin ve Milad, 2016). Bu, kimliklerinin açığa çıkmasından endişe etmeden terör örgütlerine para göndermek isteyen destekçilerine güven vermektedir. Destekçiler kripto paraları doğrudan veya bir komisyoncu aracılığıyla transfer edebilme olanağına sahiptir (Wardhana ve Nugroho, 2021).

Bunun da ötesinde, kripto paralar terör örgütlerine kara para aklama için açık bir fırsat ve olası düzenlemeleri atlamak için bir dizi seçenek sunmaktadır (Whyte, 2019). Özellikle bazı kripto paraların sınırsız ve eşler arası (P2P) doğası, terör örgütlerine, yüksek miktarda fon transfer etme ve fiat para birimine çevirme olanağı sağlamaktadır (Keatinge, Carlisle ve Keen, 2018).

Kripto paraların terör örgütleri tarafından kullanım örnekleri incelendiğinde DEAŞ ve onunla bağlantılı grupların ön plana çıktığı görülmektedir.

Her ne kadar DEAŞ terör örgütü kurulduğu ve etkili olduğu dönemde fonlarının çoğunu Irak ve Suriye'de ele geçirilen petrol sahalarından elde etse de finansmanını güvence altına almak için özellikle bağışlara güvenmiştir. Bununla birlikte, DEAŞ ile mücadele kapsamında gerekli birimler söz konusu durumun farkında olduklarından ve DEAŞ'ın aktif olarak bankacılık kanalları aracılığıyla tüm finansman çabalarını takip etmeye ve engellemeye çalıştıklarından, bağış alması da giderek zorlaşmıştır. Bu sebeple de DEAŞ, para transfer etmek için anonim ve izlenemez yollar aradığı için Bitcoin gibi kripto paraları kullanmaya başlamıştır (Charles, 2014).

Örneğin 2015 yılında ABD'nin Virginia eyaletindeki bir davada, 17 yaşındaki Ali Shukri Amin, DEAŞ destekçilerine finansal bağışları gizlemek için Bitcoin'i kullanma konusunda Twitter'da çevrimiçi tavsiyelerde bulunmaktan yargılanmıştır (Department of Justice, 2015). Ayrıca yine DEAŞ mensubu Endonezyalı bir kişi, 2016 yılında yayınladığı çevrimiçi kılavuzda, Bitcoin'i *kartlama* (sahte kredi kartı işlemleri) gelirlerini aklamak için fon taşıma yöntemlerinden biri olarak önermiştir. Aynı kişi daha sonra Endonezya'nın kolluk kuvvetleri tarafından Bitcoin kaynaklı fonlarla PayPal kullanarak ortaklarına para aktardığı ve bu paranın Temmuz 2016'da Central Java'daki Solo Polis Merkezi'nde bir intihar saldırısını finanse etmek için kullanıldığı tespit edilmiştir (Arianti ve Yaoren, 2020).

Başka bir örnekte, 2017 yılında ABD'nin New York şehrinde Pakistan asıllı ABD vatandaşı Zoobia Shahnaz adlı bir kişi, *Bitcoin üzerinden kara para aklamak ve bu parayı DEAŞ'a göndermeye çalışmakla* suçlanmıştır. Mahkeme tutanaklarında Shahnaz'ın, Ocak 2016'da Suriye Amerikan Tıp Derneği'nde gönüllü olmak için Ürdün'e gittiği, iki hafta boyunca Amman'da DEAŞ'ın önemli bir etkiye sahip olduğu Zataari Mülteci kampındaki Suriyeli mültecilere tıbbi yardım sağlanmasına yardım ettiği ifade edilmiştir. Söz konusu tutanaklarda 2017 yılının Mart ile Temmuz ayları arasında Shahnaz'ın, ABD'de çok sayıda

finans kurumunu dolandırarak 85.000 dolardan fazla yasadışı fon elde ettiği ve bu fonların bir kısmını Bitcoin ile DEAŞ'a gönderdiği de açıkça belirtilmektedir (USA v. Zoobia Shahnaz, Indictment, Case: 2:17-cr-00690, 2017; Department of Justice, 2018).

Başka bir örnekte, 2018 yılının Ekim ayında Suriye'de Tahrir El Şam'ı destekleyen Endonezyalı aşırılık yanlısı olan ancak yardım kuruluşu olduğunu iddia eden Abu Ahmed Vakfı, kripto paraları kullanarak bağış gerçekleştirdiği ifade edilmiştir. Söz konusu kurum, destekçilerini Bitcoin, Monero, Dash ve Verge gibi kripto paraları kullanarak bağış yapmaya teşvik ettiği belirtilmektedir (Arianti ve Yaoren, 2020).

Bir diğer örnek İngiltere'de 2020 yılında, DEAŞ üyesi olduğu iddia edilen Hashim Chaudhary adlı kişinin Suriye'nin kuzeyindeki hapishanelerde tutulan teröristlerin kaçmasını finanse etmek için Bitcoin kullanmasıdır. İngiltere'nin adli makamları söz konusu kişinin Bitcoin üzerinden DEAŞ için bağış toplayıp para transferlerinde bulunduğunu ifade etmiştir (Dearden, 2020).

Benzer bir örnek de 2021 yılında Rusya'da yaşanmıştır. Daha önce terör suçlarından hüküm giyen bir kişi DEAŞ üyesi olduğu ve DEAŞ'ı finanse etmek için kripto para topladığı suçlamasıyla yakalanmıştır. Yapılan soruşturma neticesinde söz konusu kişinin DEAŞ için para topladığı, dijital bir cüzdan ve kapalı bir topluluk oluşturup yönettiği açıklanmıştır (Sputniknews, 2021 Ekim 27).

Örnekler sadece DEAŞ terör örgütü ile sınırlı olmamakla birlikte, Hamas'ın askeri kanadı İzzeddin El-Kassam Tugayları da Filistin direnişine sanal para Bitcoin ile destek talebinde bulunmuştur. İzzeddin El-Kassam Tugaylarının askeri sözcüsü Ebu Ubeyde, 31 Ocak 2019'da Hamas'ın Bitcoin cinsinden bağış almaya başladığını duyurmuş ve cüzdanın bağlantısını yayınlamıştır (Emir, 2022).

Benzer şekilde PKK/PYD/YPG terör örgütünün de kripto paraları finansman maksatlı kullanma çabası içerisinde olduğuna dair örnekler de bulunmaktadır. Bitcoin kullanan kişilerin kimliğini potansiyel olarak gizleyebileceği Dark Wallet yazılımını geliştiren Amir Taaki isimli yazılımcı 2015 yılında Suriye'ye giderek PKK terör örgütünün Suriye uzantısı YPG'ye katılarak, teröristlere açık kaynaklı kod yazılımı ve karanlık ağın kullanımı hususunda eğitimler vermiştir. Taaki ile birlikte çalışan Pablo Prieto adlı bir biyolog da teröristlere karanlık ağın ve Bitcoin'in kullanımının önemini ifade etmiştir (Sönmez ve Çelik, 2020; Greenberg, 2017).

Yakın zamanda Fethullahçı terör örgütünün de (FETÖ) kripto paraları kullandığı deşifre edilmiştir. FETÖ'nün, üyelerinin itirafçı olmasını engellemek için DEAŞ terör örgütü örneğinde olduğu gibi yurt dışından para transferinde Hawala yöntemini kullandığı tespit edilmiş, transfer için toplanan 200 bin doları da kripto paralara yatırım yaparak temin ettiği ifade edilmiştir (Milliyet Gazetesi, 2022 Nisan 08). 2016 yılı öncesi söz konusu terör örgütünün daha çok borsa, Foreks ve altın piyasasında etkin olduğu, 2016 sonrasında ise kripto paraları kullanmaya çalıştığı söylenmekte ve yaklaşık 50 milyar doların üzerinde işlem hacmine sahip olduğu belirtilmektedir (Eryılmaz, 2022).

Söz konusu örnekler, terör örgütlerinin kripto paralar aracılığıyla çevrimiçi kitle yaratma çabalarıyla birlikte bağış toplama ve P2P transferlerini kullanarak fonları küresel olarak taşıma ve aktarma yeteneğine sahip olma çabası içerisinde olduklarını göstermektedir.

SONUÇ VE DEĞERLENDİRME

Terör örgütleri varlıklarını sürdürebilmek ve eylemlerini gerçekleştirebilmek için finansman kaynakları yaratma ve bu kaynaklardan elde ettiği gelirleri değerlendirerek çeşitli bölgelerdeki elemanlarına kolayca aktarabilme yöntemleri geliştirebilme zorunlulukları bulunmaktadır. Bu noktada terör örgütlerinin finansman kaynakları bakımından meşru yatırımlar, devlet sponsorluğu, bağışlar ve gasp, uyuşturucu, silah ve insan kaçakçılığı gibi çeşitli yasa dışı gelirleri bulunmaktadır. Terör örgütleri söz konusu alanlardan elde ettiği gelirleri arttırabilmek adına öncelikle kaynaklarını yönetmesi, akabinde de eylemlerini finanse edebilmek adına bu kaynakları ilgili bölge ve elemanlarına aktarması gerekmektedir. Bu aktarma işlemleri geleneksel olarak nakit kuryeler, hawala gibi gayri resmî transfer sistemleri ve resmî bankacılık işlemleri üzerinden yapılmaktadır. Ancak söz konusu yöntemler hacim ve güvenlik bakımından terör örgütlerine risk oluşturmaktadır. Özellikle 11 Eylül saldırıları sonrası finansal kurumlara ve bankacılık sektörüne yönelik düzenlemeler nedeniyle şüpheli aktarımlar tespit edilebilmekte ve yasal kanallar vasıtasıyla finanse edilen bir terör eyleminin gerçekleşme ihtimali zayıflamaktadır.

Bu noktada terör örgütleri de teknolojik gelişmelerle birlikte fonlarını yönetebilmek ve bir noktadan diğerine nasıl aktarılabilecekleri konusunda arayışlara girmiş ve özellikle son dönemlerde internet üzerinden daha kolay ve hızlı yönetim ve küresel transferler sağlayan kripto paraları kullanma eğiliminde olmuşlardır. Bu çalışma da kripto paraların takibin ve kontrolün zor olduğu internet üzerinden terör örgütleri açısından finansman yaratma ve değer aktarma avantajına sahip olduğunu iddiasından hareketle terör örgütlerinin bu paraları kullanma arayışında olmalarının altında yatan nedenleri incelemiştir.

Terör örgütlerinin kripto paraları kullanma arayışında olmalarının temel sebebi, bu paraların fiat para birimlerine göre anonimliğe sahip olmasıdır. Kripto paraların, bir banka veya finans kurumu gibi bir üçüncü tarafa güvenmeden ağ etkinliği hakkında fikir birliği sağlayan açık kaynaklı P2P değer aktarım ağlarına ve bu ağlara erişimi sağlayan özel anahtarlı para cüzdanlarına sahip olması, ayrıca Dark Wallet gibi kripto paraları kullanan kişilerin kimliğini potansiyel olarak gizleyebileceği programların geliştirilmesi bu anonimliğin oluşmasını sağlamıştır.

Kripto paralardaki bu anonimlik, belirli dönemlerde değer artışlarıyla ve hukuksal boşluklarla birleştiğinde, terör örgütleri için çekicilik doğurmuştur. Çalışmada incelenen örnekler, şu an için kripto paraların bağış toplamak, eylemleri finanse etme amaçlı para aktarmak ve gelirleri yönetmek maksatlı kullanıldığını göstermektedir.

Ancak terör örgütleriyle mücadele eden kolluk kuvvetleri açısından asıl risk, terör örgütlerinin karanlık ve derin ağı, kredi kartı bilgilerini elde etmek, pasaport gibi sahte belgeler temin etmek, silah/mühimmat satın almak ve uyuşturucu satışı yapmak gibi amaçlar doğrultusunda kripto paralar üzerinden kullanmaya başlamalarıdır. Karanlık ve derin ağdan kripto paralar ile alışveriş yapılabilmesinin, özellikle yasa dışı finansman kaynaklarına erişim imkânı olmayan *yalnız kurt* teröristlerine avantaj sağlayabileceği ve *bireysel* terör eylemlerinde artışlar yaşanabileceği düşünülmektedir.

Sonuç olarak internetin genişleyen ve gelişen ölçeği ile doğru orantılı bir şekilde terör örgütleri de eylemleri için yeni finansman kaynakları yaratmak, para aktarmak ve gelirlerini yönetmek için interneti kullanmaya devam edeceklerdir. Bu noktada, kripto paralar gibi terör örgütlerinin yeni finansman unsurlarına karşı önlem alınması için küresel çapta yasal tedbirler alınması ve devletler arasında iş birliği yapılması gerekmektedir.

Etik Beyanı: *Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazarlar beyan eder. Aksi bir durumun tespiti halinde Türk Sosyal Bilimler Araştırmaları Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarlarına aittir.*

Yazar Katkıları: *1. yazar ve 2. yazar çalışmada makalenin bütününe katkı sağlamıştır. 1. yazarın katkı oranı: %50, 2. yazarın katkı oranı: %50'dir.*

Çıkar Beyanı: *Yazarlar arasında çıkar çatışması yoktur.*

KAYNAKLAR

Aly, A., Macdonald, S., Jarvis, L. ve Chen, T. M. (2017). Introduction to the special issue: Terrorist online propaganda and radicalization, *Studies in Conflict & Terrorism*, 40 (1), 1-9.

Arianti, V., ve Yaoren, K. Y. (2020). How terrorists use cryptocurrency in Southeast Asia, *The Diplomat*, 10 Ekim 2022 tarihinde https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia/ adresinden alındı.

Başaranel, B. U. (2021). Derin ağ. İçinde N. Akdemir ve C. O. Tuncer (Ed.), *Siber ansiklopedi: Siber ortama çok disiplinli bir yaklaşım*. Ankara: Pegem Akademi Yayıncılık.

Biersteker, T. J., ve Eckert, S. E. (2008). Introduction: the challenge of terrorist financing, İçinde Thomas J. Biersteker ve Sue E. Eckert (Ed.), *Countering the Financing of Terrorism*, New York: Routledge.

Biswas, B., ve Sana, A. K. (2019), Issues in terrorism financing: An analysis, İçinde Ramesh Chandra Das (Ed.) *The Impact of Global Terrorism on Economic and Political Development: Afro-Asian Perspectives*, Emerald Publishing Limited.

Carroll, P., ve Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future, *Journal of Policing, Intelligence and Counter Terrorism*, 13 (3), 285-300.

Charles, B. S. (2014). ISIS. Are they using bitcoins to fund criminal activities?, *Security Intelligence*, 12 Ekim 2022 tarihinde https://securityintelligence.com/isis-are-they-using-bitcoins-to-fund-criminal-activities/ adresinden alındı.

Chêne, M. (2008). Hawala remittance system and Money laundering, 15 Ekim 2022 tarihinde https://www.u4.no/publications/hawala-remittance-system-and-money-laundering.pdf adresinden alındı.

Clarke, C. P., ve Williams, P. (2018). Da'esh in Iraq and Syria: Terrorist criminal enterprise. İçinde Kimberley L. Thachuk ve Rollie Lal (Ed.), *Terrorist Criminal Enterprises: Financing Terrorism through Organized Crime*. Praeger Security International.

Conway, M. (2006). Terrorist use of the internet and fighting back, *Information & Security: An International Journal*, 19, 9-30.

Copestake, J. (2014). Hiding currency in the dark wallet, *BBC*, 20 Ekim 2022 tarihinde https://www.bbc.com/news/technology-29283124 adresinden alındı.

Çarkacıoğlu, A. (2016). Kripto-para bitcoin, *Sermaye Piyasası Kurulu Araştırma Dairesi*, Araştırma Raporu.

Dearden, L. (2020). Isis member used Bitcoin to transfer money from UK for release of jihadists in Syrian prisons court hears, *Independent*, 01 Kasım 2022 tarihinde https://www.independent.co.uk/news/uk/crime/isis-uk-prison-syria-bitcoin-hashim-chaudhary-b1639224.html adresinden alındı.

Department of Justice. (2018). New York Woman Pleads Guilty to Providing Material Support to ISIS, 11 Kasım 2022 tarihinde https://www.justice.gov/opa/pr/new-york-woman-pleads-guilty-providing-material-support-isis adresinden alındı.

Department of Justice. (2015). Virginia Teen Pleads Guilty to Providing Material Support to ISIL, 12 Kasım 2022 tarihinde https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil adresinden alındı.

Eğilmez, M. (2017). Kripto Paralar, Bitcoin ve Blockchain, *Kendime Yazılar*, 09 Kasım 2022 tarihinde https://www.mahfiegilmez.com/2017/11/kripto-paralar-bitcoin-ve-blockchain.html adresinden alındı.

Emir, A. E. (2022). Hamas plans to continue using cryptocurrencies for operations, *Al-monitor*, 11 Kasım 2022 tarihinde https://www.al-monitor.com/originals/2022/01/hamas-plans-continue-using-cryptocurrencies-operations#ixzz7m7pYvfXC adresinden alındı.

Eryılmaz, F. (2022). İstihbarat ve terör örgütlerinde kripto para dönemi, *Kriter*, 6 (64), 13 Kasım 2022 tarihinde https://kriterdergi.com/dosya-turkiyede-ve-dunyada-istihbarat/istihbarat-ve-teror-orgutlerinde-kripto-para-donemi adresinden alındı.

Financial Action Task Force (2008). Terrorist financing, *FATF/OECD*, 12 Kasım 2022 tarihinde https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf adresinden alındı.

Freeman, M. (2011). The sources of terrorist financing: theory and typology, *Studies in Conflict & Terrorism*, 34, 461-475.

Freeman, M., ve Ruehsen, M. (2013). Terrorism financing methods: An overview, *Perspectives on Terrorism*, 7(4), 5-26.

Gediz Oral, B., ve Yeşilkaya, Y. (2021). Kripto para ikilemi: Karapara aklama ve bitcoin. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 39, 209-239.

Goldman, Z. K., Maruyama, E., Rosenberg, E., Saravalle, E. ve Strauss, J. S. (2017). Terrorist use of virtual currencies, *Center for a New American Security*, 11 Kasım 2022 tarihinde https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies adresinden alındı.

Greenberg, A. (2017). How an anarchist bitcoin coder found himself fighting ISIS in Syria, *Wired*, 12 Kasım 2022 tarihinde https://www.wired.com/2017/03/anarchist-bitcoin-coder-found-fighting-isis-syria/ adresinden alındı.

Hinnen, T. (2004). The cyber-front in the war on terrorism: Curbing terrorist use of the internet. *Columbia Science and Technology Law Review*, 5, 1-42.

IMF. (2022). Anti-Money Laundering/Combating the Financing of Terrorism-Topics, 20 Kasım 2022 tarihinde https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm#financingterrorism adresinden alındı.

INTERPOL (2022). Tracing terrorist finances, 21 Kasım 2022 tarihinde https://www.interpol.int/Crimes/Terrorism/Tracing-terrorist-finances adresinden alındı.

Irwin, A. S. M. ve Milad, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control*, 19(4), 407-425.

İşler, B., Takaoğlu, M. ve Küçükali, U. F. (2019). Blokzinciri ve kripto paraların insanlığa etkileri, *Yeni Medya Elektronik Dergisi*, 3 (2), 71-83.

Jacobson, M. (2010). Terrorist financing and the internet, *Studies in Conflict & Terrorism*, 33 (4), 353-363.

Jost, P. M. ve Sandhu, H. S. (2013). The hawala alternative remittance system and its role in money laundering, *INTERPOL/FOPAC*, 25 Kasım 2022 tarihinde https://www.assetsearchblog.com/wp-content/uploads/sites/197/2013/06/FinCEN-Hawala.pdf adresinden alındı.

Karaman, A. (2021). Bitcoin mixer nedir? Karıştırıcılar neden yasak?, 25 Kasım 2022 tarihinde https://tr.cointelegraph.com/news/what-are-bitcoin-mixers-why-are-they-banned adresinden alındı.

Keatinge, T., Carlisle, D. ve Keen, F. (2018). Virtual currencies and terrorist financing: assessing the risks and evaluating responses, Directorate General for Internal Policies Policy Department for Citizens' Rights and Constitutional Affairs.

Kfir, I. (2020). Cryptocurrencies, national security, crime and terrorism, *Comparative Strategy*, 39(2), 113-127.

Milliyet Gazetesi. (2022 Nisan 08). FETÖ'nün para trafiği deşifre oldu, *Milliyet*, 27 Kasım 2022 tarihinde https://www.milliyet.com.tr/gundem/fetonun-para-trafigi-desifre-oldu-6733791 adresinden alındı.

Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System, 20 Kasım 2022 tarihinde https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf adresinden alındı.

Nian, L. P. ve Chuen, D. L. K. (2015). Introduction to Bitcoin, İçinde David Lee Kuo Chuen (Ed.), *Handbook of Digital Currency*, New York: Elsevier.

Normark, M. ve Ranstorp, M. (2015). Understanding Terrorist Finance Modus Operandi and National CTF-Regimes, *SEDU Designation* 22 Kasım 2022 tarihinde https://www.fi.se/contentassets/1944bde9037c4fba89d1f48f9bba6dd7/understanding_terrorist_finance_160315.pdf adresinden alındı.

Paoli, G. P., Aldridge, J., Ryan, N. ve Warnes, R. (2017). Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web, *RAND Corporation*, 21 Kasım 2022 tarihinde https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf adresinden alındı.

Patel, P. C., ve Pereira, I. (2021). The relationship between terrorist attacks and cryptocurrency returns, *Applied Economics*, 53(8), 940-961.

Raphaeli, N. (2003). Financing of Terrorism: Sources, methods, and channels, *Terrorism and Political Violence*, 15 (4), 59-82.

Schott, P. A. (2006). Reference guide to anti-money laundering and combating the financing of terrorism, *The World Bank*, 21 Kasım 2022 tarihinde https://documents1.worldbank.org/curated/ar/558401468134391014/pdf/350520Referenc1Money01OFFICIAL0USE1.pdf adresinden alındı.

Schwarz, C. D., Manheim, D. ve Johnston, P. B. (2019). *Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats*, Santa Monica: RAND Corporation.

Schwarz, N., Chen, K., Poh, K., Jackson, G. vd. (2021). Virtual assets and anti-money laundering and combating the financing of terrorism, *International Monetary Fund*, 25 Kasım 2022 tarihinde https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654 adresinden alındı.

Sönmez, G., ve Çelik, E. (2020). Anonimlik ile illegalite arasında: Deep web, dark web ve devlet dışı silahlı aktörlerin uluslararası siber faaliyetleri. *Güvenlik Çalışmaları Dergisi*, 22 (1), 66-88.

Sputniknews. (2021 Ekim 27). Rusya'da IŞİD için kripto para toplayan bir kişi yakalandı, *Sputnik Türkiye*, 21 Kasım 2022 tarihinde https://sputniknews.com.tr/20211027/rusyada-isid-icin-kripto-para-toplayan-bir-kisi-yakalandi-1050226562.html adresinden alındı.

Thachuk, K. L. ve Lal, R. (2018). An Introduction to terrorist criminal enterprises. İçinde Kimberley L. Thachuk ve Rollie Lal (Ed.), *Terrorist Criminal Enterprises: Financing Terrorism through Organized Crime*. Praeger Security International.

The United Nations (1999). International convention for the suppression of the financing of terrorism, 25 Kasım 2022 tarihinde https://treaties.un.org/doc/db/terrorism/english-18-11.pdf adresinden alındı.

Türkşen, U. (2021a). Karanlık Ağ. İçinde N. Akdemir ve C. O. Tuncer (Ed.), *Siber ansiklopedi: Siber ortama çok disiplinli bir yaklaşım*. Ankara: Pegem Akademi Yayıncılık.

Türkşen, U. (2021b). Kripto Para Birimleri. İçinde N. Akdemir ve C. O. Tuncer (Ed.), *Siber ansiklopedi: Siber ortama çok disiplinli bir yaklaşım*. Ankara: Pegem Akademi Yayıncılık.

USA v. Zoobia Shahnaz, Indictment, Case: 2:17-cr-00690. (2017). United States District Court for the Eastern District of New York, 26 Kasım 2022 tarihinde https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Zoobia%20Shahnaz%20AUSA%20bail%20letter%2012-14-17.pdf adresinden alındı.

Wardhana, A. T. ve Nugroho, B. W. (2021). Abuse of cryptocurrency to funding international terrorism activities, *Engaging Youth in Community Development to Strengthen Nation's Welfare*, 1(1), 18 Kasım 2022 tarihinde https://prosiding.umy.ac.id/grace/index.php/pgrace/article/view/190 adresinden alındı.

Whyte, C. (2019). Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise, *Studies in Conflict & Terrorism*, 1-24

Wilkinson, P. (2005). International terrorism: the changing threat and the EU's response, *Institute for Security Studies*, No: 84, 20 Kasım 2022 tarihinde https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp084.pdf adresinden alındı.

Windle, J. (2018). Fundraising, Organised Crime and Financing Terrorism. İçinde A. Silke (Ed.), *The Routledge Handbook of Terrorism and Counterterrorism*. Abingdon: Routledge.

Wolf, S. O. (2021). Terrorism financing: Crypto-Taliban?, *SADF Comment*, No. 217, 25 Kasım 2022 tarihinde https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3941105 adresinden alındı.