Üçüncü Sektör Sosyal Ekonomi Dergisi
Third Sector Social Economic Review
57(4) 2022, 3229-3241
doi: 10.15659/3.sektor-sosyal-ekonomi.22.12.2018

Araştırma Makalesi

Terörizmin Finansmanında Siber Tehditler ve Kripto Paraların Rolü

Cyber Threats and the Role of Crypto Currencies in the Financing of Terrorism

Oğuzhan Yanarışık
Dr. Öğretim Üyesi, Polis Akademisi
Güvenlik Bilimleri Enstitüsü
yanarisik@gmail.com
https://orcid.org/0000-0003-3442-4779

Makale Geliş Tarihi	Makale Kabul Tarihi
09.11.2022	**12.12.2022**

Öz

Teröristler, militan toplamak ve desteklemek, lojistik merkezler kurmak ve yönetmek ve operasyonları yürütmek için finansmana ihtiyaç duymaktadır. Bu kapsamda, terörist gruplar, faaliyetlerini finanse etmek için interneti ve sanal dünyayı yaygın bir şekilde kullanmaktadır. Doğrudan internet üzerinden bağış toplayarak, elektronik ticaret yaparak, çevrimiçi kumar faaliyetleri yürüterek, online ödeme sistemlerini manipüle ederek, dijital para çalarak, Dark Web'de uyuşturucu ve yasa dışı ürünler satarak veya hayır kurumu benzeri yapıları istismar ederek önemli finansal kaynaklar elde etmektedir. İnternet ve mobil teknolojilerin sağladığı teknolojik imkanlar terör örgütlerinin kara para aklamasına da yardım etmektedir. Bitcoin benzeri kripto para birimleri veya Linden Doları benzeri sanal paralar, bu örgütlerin gizlice para transfer etmesine olanak tanımaktadır. Bu çalışmada, terörizmin finansmanında ve bununla mücadelede siber tehditlerin ve kripto paraların rolü analiz edilmektedir. Bu çalışma, çeşitli makalelerden, araştırma çalışmalarından ve web sitelerinden ikincil veri toplama yoluyla kripto para biriminin terörizmin finansmanındaki etkisini incelemektedir. Kripto paralar merkezi olmayan para birimleri olduğundan ve işleyişinde büyük bir anonimlik olduğundan dolayı, kullanımını takip etmek oldukça zordur. Bu da çalışmada birincil veri tabanı araştırması yapmayı zorlaştırmaktadır. Dolayısıyla, bu çalışmada terörün finansmanı ve kripto paranın ilişkisinin değerlendirilmesi kamuya açık olan bilgilerle yapılmaktadır.

Anahtar Kelimeler: *Terörizmin Finansmanı, Uluslararası Güvenlik, Kripto Paralar, Siber Tehditler*

Abstract

Terrorists need funding to recruit and support militants, set up and manage logistics centers, and run operations. In this context, terrorist groups widely use the internet and virtual world to finance their activities. They obtain significant financial resources by collecting donations directly on the Internet, conducting electronic commerce, conducting online gambling activities, manipulating online payment systems, stealing digital currency, selling drugs and illegal products on the Dark Web, or exploiting charity-like structures. The technological opportunities provided by the Internet and mobile technologies also help terrorist organizations to launder money. Cryptocurrencies like Bitcoin or virtual currencies like the Linden Dollar allow these organizations to transfer money secretly. In this study, the role of cyber threats and cryptocurrencies in financing and combating terrorism is analyzed. This study examines the impact of cryptocurrency on terrorism financing through secondary data collection from various articles, research studies and websites. Since cryptocurrencies are decentralized currencies and there is great anonymity in their operation, its usage is quite difficult to track. This makes it difficult to conduct a primary database search in the study. Therefore, in this study, the evaluation of the relationship between terrorist financing and crypto money is made with publicly available information.

Önerilen Atıf /Suggested Citation
Yanarışık, O., 2022 Terörizmin Finansmanında Siber Tehditler ve Kripto Paraların Rolü, *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 57(4), 3229-3241

Keywords: *Financing of Terrorism, International Security, Crypto Currencies, Cyber Threats*

1. Giriş

Terör faaliyetleri, münferit eylemlerden organize grupların planlı faaliyetlerine kadar çok farklı şekillerde gerçekleşmektedir. Dolayısıyla terörün finansman biçimleri de buna göre değişmektedir. Terör örgütleri, hem terör eylemlerinin fiilen gerçekleştirilebilmesi için hem de örgütün işleyişini sürdürmek, temel teknik gereksinimlerini sağlamak ve ideolojilerinin yayılmasıyla ilgili maliyetleri karşılamak için önemli fonlara ihtiyaç duymaktadır. Terörist grupların ayakta kalabilmeleri ve terör eylemleri gerçekleştirebilmeleri için paraya ihtiyaçları vardır. Terörün finansmanı, terör örgütlerinin faaliyetlerini finanse etmek için kullandıkları araç ve yöntemleri kapsamaktadır. Bu para, legal görünümlü işletmelerden ve hayır kurumlarından elde edilen kârlar gibi meşru algılanan kaynaklardan gelebilmektedir. Bunun yanında terörist gruplar, silah, uyuşturucu veya insan kaçakçılığı, yasadışı emtia ticareti (petrol, kömür, elmas, altın ve narkotik) veya fidye için adam kaçırma gibi yasa dışı faaliyetlerden de finansman sağlayabilmektedir. Son dönemde, terörün finansmanında siber dünyanın ve kripto paraların rolü giderek artmaktadır. Çünkü nakit para kullanımı gibi geleneksel yöntemler arkasında iz bırakmaktadır ve daha kolay takip edilebilmektedir (Bantekas, 2003, s. 319).

Terörizm, son birkaç on yılda istikrarlı bir şekilde organize suçla entegre olmuştur. Bu, bir bakıma terörist grupların 21. Yüzyılın yeni şartlarına uyum sağlama yeteneğini göstermektedir. Gizli operatörlere ödeme yapılması ve silah ve patlayıcıların satın alınması da dahil olmak üzere günümüzde terör operasyonlarının finansmanı, yalnızca yasa dışı operasyonların karşılayabileceği türde işlemleri gerektirmektedir. Bu itibarla, terörist suç girişimlerine doğru evrim, yalnızca birçok terörist grubun hayatta kalmasını ve büyümesini sağlamakla kalmamış, aynı zamanda onlara daha fazla esneklik ve hareketlilik kazandırmıştır (Thachuk ve Lal, 2018, s. 1). Genellikle uyuşturucu kaçakçılığı, soygun veya gasp gibi diğer ciddi suçların bir bileşeni olan ve yasa dışı yollarla elde edilen gelirlerin kaynağının meşru kaynaklardan gelmiş gibi görünmesi için gizlenmesini ifade eden kara para aklama gibi faaliyetler oldukça yaygınlaşmıştır. Günümüzün dinamik operasyon ortamında dönüşen terör tehdidiyle başa çıkmak, aşırılık yanlısı grupların neden organize suça yöneldiklerini, gelişen suç işlerine nasıl başladıklarını ve politika yapıcıların yeni tehditle mücadele etmek için neler yapabileceklerini anlamayı gerektirmektedir.

Uluslararası Kriminal Polis Teşkilatı (Interpol), "internetin küresel doğasının suçluların dünyanın herhangi bir yerinde hemen hemen her türlü yasa dışı faaliyette bulunmalarına izin verdiğini ve bunun da tüm ülkelerin siber uzayda işlenen suçları kapsamak için kendi yerel çevrimdışı kontrollerini sağlamalarını zorunlu kıldığını" belirtmektedir (Kerr, 2003, s. 372-373). Bu nedenle Interpol, bu yeni suç faaliyeti dalgasıyla mücadele etmek için yerel hükümetlerin yerel gerçek dünya yasalarını siber uzayda işlenen suçlara uyacak şekilde uyarlamaları gerektiğini vurgulamaktadır. ABD Federal Soruşturma Bürosu'nun raporuna göre, sadece 2021 senesinde İnternet Suçları Şikâyet Merkezi'ne intikal eden 847,376 şikâyete konu olan siber suçların toplam maliyeti 6 trilyon ABD Dolarını aşmıştır (FBI, 2022, s. 7). 2025 yılına gelindiğinde, siber suçların küresel yıllık maliyetinin 10,5 trilyon ABD Dolarına ulaşacağı tahmin edilmektedir (Morgan, 2020). Terör örgütleri bu büyük pastadan pay kapabilmek için birbiriyle yarışmaktadır.

Paranın kaynağına ilişkin hiçbir bilgi bulundurmadığından ve gerektiğinde sahibi tarafından nakit paraya dönüştürülebildiğinden ve alınıp satılabildiğinden dolayı kripto paralar, yasadışı faaliyetleri ve terörizmi destekleyebilmektedir. Kripto paralar, akıllı bilgisayar korsanları tarafından manipüle edilebilecek ve siber saldırılara imkân verecek dijital platformlarda çalışmaktadır. Son zamanlarda, terörizm, kripto para birimleri ile eş zamanlı olarak büyümektedir. Geçmişten günümüze geldikçe, küresel terör hacminin kripto paralarla paralel şekilde genişlediği görülmektedir. 2000-2002, 2006-2008, 2012-2014 ve 2016-2017 yılları arası küresel ölçekli terörün zirve yaptığı göz önünde bulundurulduğunda, kripto para ile terör arasında doğrudan bağlantı ve bir korelasyon olduğu öne sürülebilir (Majumder, Routh ve Singha, 2019, s. 132-133).

Birleşmiş Milletler bünyesinde hazırlanan Terörün Finansmanının Önlenmesine Dair Uluslararası Sözleşme'de, terörizm eylemlerinin tüm biçimlerinde ve tezahürlerinde dünya çapında yükselmesi konusunda derin endişe duyulduğu belirtilmekte ve terörizmin finansmanının uluslararası toplum için ciddi bir tehlike kaynağı olduğu vurgulanmaktadır. Uluslararası terörizmin eylemlerinin sayısının ve

ciddiyetinin, teröristlerin elde edebileceği finansmana bağlı olduğunu belirtilmektedir. Terörizmin finansmanının önlenmesi ve faillerinin kovuşturulması ve cezalandırılması yoluyla bastırılması için etkili önlemlerin tasarlanması ve benimsenmesinde uluslararası iş birliğini geliştirme ihtiyacına imzacı devletlerin ikna olduğu ifade edilmektedir (Birleşmiş Milletler, 1999).

Sanal alemde terörist örgütlerin varlığı yeni bir durum değildir. Teröristler ilk kuruluş döneminden beri internetin imkânlarından istifade etmeye gayret etmektedir. Örneğin, 1998 senesinde Amerika Birleşik Devletleri tarafından terör grupları listesine eklenen otuz örgütün yaklaşık yarısının kendi web sitesi vardır. Günümüzdeyse büyüklükleri, faaliyet alanları ve yetenekleri her ne seviyede olursa olsun hemen hemen bütün faal terör örgütleri siber dünyada bir şekilde varlıklarını devam ettirmektedir. Bazılarının farklı alanlara odaklanan çok dilli ve çeşitli web siteleri bulunmaktadır. Ayrıca, hemen hemen hepsi online sohbet odalarında, sosyal ağ ortamlarında, forumlarda ve gizlice topluma ulaşmalarına yarayacak diğer halka açık platformlarda yer almaktadır (Dilipraj, 2019, s. 77-83).

Teknolojinin gelişmesiyle birlikte siber dünya terörizmin finansmanında çok ciddi bir mecra haline gelmiştir. Bir başka ifadeyle, terör örgütleri ve destekçileri interneti terör eylemlerini finanse etmek için sürekli artan bir oranda kullanmaktadır. Teröristlerin fon ve kaynak toplamak için interneti kullanma biçimleri dört genel kategoride sınıflandırılabilir: Destekçilerinden doğrudan finansman talep etme, e-ticaret sitelerini istismar etme, çevrimiçi ödeme araçlarını istismar etme ve hayır kurumlarını istismar etme (Birleşmiş Milletler Uyuşturucu ve Suç Ofisi, 2012, s. 7).

Terör örgütleri tarafından para toplamak veya mal satın almak için kripto para birimlerinin kullanıldığına dair kanıtlar vardır. Bununla birlikte, bu kanıtlar "genel olarak doğrulanmamış ve anekdot niteliğinde" olma eğilimindedir. Ayrıca, belirtilen vakalar nispeten azdır ve nispeten küçük miktarlarda gelir içermektedir (Carroll ve Windle, 2018, s. 289). Çünkü kripto paraların izini sürmek ve onları terörist faaliyetlerle ilişkilendirmek oldukça güçtür. Bununla birlikte, Wall'un (2005, s. 81) belirttiği üzere, internet, "yalnız (tekil) suçlulara..." küresel ölçekte sayısız kez tekrarlanabilecek inanılmaz derecede karmaşık ve geniş kapsamlı görevleri yerine getirme yeteneği kazandırarak, suç faaliyetinin örgütsel doğasını değiştirmiştir. Bu nedenle, yalnız kurt siber finansörler olarak adlandırılabilecek bir kavramın ortaya çıkışını görmemiz mümkündür: Herhangi bir fiziksel terörist hücreyle bağlantısı olmayan kişiler, terörizme yardım etmek için suç faaliyeti yoluyla para toplayabilmektedir.

Bu çalışmada, terörizmin finansmanında ve bununla mücadelede siber tehditlerin ve kripto paraların rolü analiz edilmektedir. Bu çalışma, çeşitli makalelerden, araştırma çalışmalarından ve web sitelerinden ikincil veri toplama yoluyla kripto para biriminin terörizmin finansmanındaki etkisini incelemektedir. Kripto paralar merkezi olmayan para birimleri olduğundan ve işleyişinde büyük bir anonimlik olduğundan dolayı, kullanımını takip etmek oldukça zordur. Bu da çalışmada birincil veri tabanı araştırması yapmayı zorlaştırmaktadır. Dolayısıyla, bu çalışmada kamuya açık olan bilgilerle terörün finansmanı ve kripto paranın ilişkisinin değerlendirilmesi yapılmaktadır.

2. Kavramsal Çerçeve: Terörizmin Finansmanı ve Siber Tehditler

Tekil terör saldırılarının maliyetleri, stratejik düzeydeki saldırılar için bile nispeten düşük olabilmektedir. Örneğin, 1993 Dünya Ticaret Merkezi saldırısının maliyetinin yaklaşık 19.000 ABD Doları olduğu tahmin edilmektedir. 2002 Bali bombalamalarının 20.000 ABD Dolarına ve 2004 Madrid saldırılarının 10.000 ila 50.000 ABD Dolarına mal olduğu düşünülmektedir. Diğer saldırılarla karşılaştırıldığında daha pahalı olduğu görülen 11 Eylül 2001 saldırılarının maliyetinin ise 350.000 ila 500.000 ABD Doları arasında olduğu değerlendirilmektedir (Freeman, 2011, s. 467).

Her ne kadar çoğu terörist saldırı nispeten ucuz olsa da bir terör örgütünü yönetmek maliyetli olabilmektedir. Özellikle de uzun süreli faaliyet yürüten gruplar veya yetkileri altındaki alanlarda devlet işlevlerini üstlenmeye çalışan örgütler için durum budur. Örneğin, sızdırılan belgeler, 2014'te Irak ve Şam İslam Devleti'nin (DEAŞ) faaliyet göstermek için ayda yaklaşık 5 milyon ABD Doları'na ihtiyaç duyduğunu göstermektedir (Cooper, 2017). Teröristler, militan toplamak ve desteklemek, lojistik merkezler kurmak ve yönetmek ve operasyonları yürütmek için de finansmana ihtiyaç duymaktadır. Bu nedenle, teröristlerin finansal kaynaklara erişimini engellemek, terör tehdidine başarılı bir şekilde karşı koymak için oldukça önemlidir. Bununla birlikte, birçok devlet, terörün finansmanı vakalarını tespit etmek, soruşturmak ve kovuşturmak için gereken yasal ve operasyonel çerçevelere ve teknik uzmanlığa sahip değildir. 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanun'un dördüncü

maddesine göre, terörizm faaliyetlerinin "gerçekleştirilmesinde tümüyle veya kısmen kullanılması amacıyla veya kullanılacağını bilerek ve isteyerek belli bir fiille ilişkilendirilmeden dahi bir teröriste veya terör örgütlerine fon sağlayan veya toplayan kişiler", terörün finansmanı suçunu işlemiş sayılmaktadır. Bu kanun kapsamında "ceza verilebilmesi için fonun bir suçun işlenmesinde kullanılmış olması şartı" aranmamaktadır (Resmî Gazete, 2013).

11 Eylül 2001 terör saldırıları öncesinde terörizmin finansmanıyla mücadelede ülkelerin yetersiz ve hatta duyarsız kaldığı yönünde eleştiriler mevcuttur. Örneğin, ABD yönetimi yaptığı açıklamada şöyle demektedir: "11 Eylül'den önce, terörizm finansörlerine ve terörü finanse eden ağlara dokunulmadı ve uluslararası toplum tarafından büyük ölçüde görmezden gelindi. Bugün, terörizmin finansmanını engellemek için dünya çapındaki saldırgan kampanyamızı sürdürerek, El Kaide ve diğer terörist grupların dünya çapında para toplamasını ve hareket ettirmesini daha zor, daha maliyetli ve daha riskli hale getiriyoruz" (Biersteker ve Eckert, 2008, s. 289). Bununla birlikte, 11 Eylül saldırıları öncesinde de terörizmin finansmanıyla ilgili bazı uluslararası zemin oluşturma çabalarının varlığından söz etmek mümkündür. Örneğin 1999 tarihli Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme, herhangi bir kişinin herhangi bir şekilde, doğrudan veya dolaylı olarak, hukuka aykırı ve isteyerek, tamamen veya kısmen, bir terör eylemi gerçekleştirmek için kullanılması kastıyla veya kullanılacağını bilerek fon sağlaması veya toplaması durumunda suç işlemiş olacağını deklare etmektedir (Schott, 2006, s. I-4).

11 Eylül saldırıları sonrasında ise bu konudaki çabalar artmış ve Birleşmiş Milletler Güvenlik Konseyi, teröre karşı önlemlerin kabul edilmesi için tartışmaların odak noktası haline gelmiştir. Alınan kararlarda, terörle ilgili fonların tespit edilmesi ve dondurulması için devletleri özel tedbirler uygulamaya mecbur bırakarak, terörün finansmanına vurgu yapılmıştır. Bu yeni önlemler, yerel ve uluslararası mali sistemlerin terörizmin finansmanıyla mücadeledeki yetersizliğini ortaya çıkarmıştır. Dahası, devletlerin kendi aralarında ve devletler, hükümetler arası kuruluşlar ve özel finans kurumları arasında koordinasyon eksikliğini ortaya koymuştur. Bu koordinasyon problemini çözmek için bazı adımlar atılmıştır. Örneğin, BM Güvenlik Konseyi 1373 sayılı kararını yayınlamış ve tüm üye devletlerden terör örgütlerinin fonlarını ve varlıklarını dondurmaları istenmiştir. 1373 sayılı kararın uygulanmasını izlemek amacıyla aynı kararda Terörle Mücadele Komisyonu kurulmuştur. Bütün devletler 1373 sayılı kararı uygulamak için attıkları adımları komiteye bildirmekle yükümlü tutulmuştur (Ilbiz, 2019, s. 4).

Terör örgütleri finansman toplamak için yasal görünümlü ve illegal birçok yöntemi kullanabilmektedir (Bantekas, 2003, s. 316). Örneğin, hayır kurumları kisvesi altında bağış toplamak için kâr amacı gütmeyen kuruluşları kullanan pek çok terör örgütü vardır. Çok sayıda bağışçıya ulaşma ve hızlı bir şekilde önemli miktarda para toplama fırsatları sağlayan bağış toplama web siteleri, aslında meşru olan bu bağış toplama yöntemini terörist ve aşırılık yanlısı örgütler için çekici kılmaktadır. Gelir elde etmenin legal görünümlü diğer yolları arasında e-ticaret platformlarında çevrimiçi ürün satışı, üyelik ücretleri ve bağlı STK'lar tarafından düzenlenen etkinlikler için yayın ve bilet satışı sayılabilir. Bunların yanında terörist gruplar, uyuşturucu dağıtımı ve satışından soygunlara, hırsızlıklara ve haraçlara kadar çeşitli illegal faaliyetlerle de finansman sağlamaktadır. Terörist ve aşırılık yanlısı aktörler, vergi sahtekarlığı ve vergi kaçakçılığı, sosyal yardım, sigorta ve kredi sahtekarlığı da dahil olmak üzere, para toplamak için çeşitli sahtekarlıklara başvurmaktadır (Europol, 2022, s. 17-19). Bütün bunları yaparken de internet, dijital para birimleri, kripto para birimleri ve sanal varlık hizmet sağlayıcılarının kullanımı, çok yüksek bir anonimlik seviyesi ve hareket kabiliyeti sağlayarak teröristlerin işini kolaylaştırmaktadır.

Bugün internet kullanıcısı sayısı 4,5 milyarı; sosyal medya kullanıcı sayısı 3,8 milyarı; cep telefonu kullanıcı sayısı ise 5,1 milyarı aşmış durumdadır. Ortalama bir internet kullanıcısı günde vaktinin yaklaşık 6 saat 43 dakikasını, yani yılda 100 günden fazlasını internette geçirmektedir (WeAreSocial ve Hootsuiye, 2020). Kovid-19 pandemisi süreci bu istatistikleri çok daha yukarı taşımıştır. Daha önceleri çoğunlukla çevrimdışı ortamda gerçekleştirilen pek çok faaliyet, artık çevrimiçi ortamda yürütülmektedir. Bu genişleyen sanal evrende güvenliği sağlayabilmek, devletler, şirketler, kurumlar ve bireyler için daha fazla önem taşımaya başlamıştır. Siber güvenlik hem iç hem de dış güvenliğin vazgeçilmez unsurlarından biri haline gelmiştir (Yanarışık, 2020, s. 304).

Siber dünya, sınırlar arasında sanal bir köprü sağlayarak, suçların daha büyük ölçekte, daha hızlı ve daha fazla geri dönüş potansiyeli ile yürütülmesine izin vermektedir. Sonuç olarak, siber mağduriyetin boyutu ve çevrimiçi kaçak mal satışları sürekli artmaktadır. Siber alem kredi kartı dolandırıcılığı, uyuşturucu ticareti, haraç, yasa dışı silah ve mühimmat alışverişi, kimlik hırsızlığı, kara para aklama ve savunmasız insanların suç faaliyetlerinde istismar edilmek üzere çevrimiçi kontrolü gibi gerçek hayatta da yürütülen illegal faaliyetler için uygun zemin oluşturabilmektedir (Carroll ve Windle, 2018, s. 287).

İnternetin terörist amaçlar için kullanılması, ulusal sınırları aşarak, mağdurlar üzerindeki potansiyel etkiyi artırmaktadır. Weimann (2006: 624) interneti terör örgütleri için cazip hale getiren etmenleri şöyle sıralamaktadır: Kolay erişim sağlaması; potansiyel olarak geniş kitlelere erişim sağlaması; düzenleme, sansür veya diğer hükümet denetimi şekillerinin çok az olması veya hiç olmaması; geleneksel kitle iletişim araçlarına olan bağımlılığı azaltması; iletişimin anonim olması ve hızlı bilgi akışı sağlaması; internette yer almanın oldukça ekonomik olması ve etkileşimli bir multimedya ortamı sağlaması.

Teknoloji, terör örgütleri ve destekçileri tarafından terörün finansmanı, militan devşirme, terör propagandası, terörist eğitimi, terör eylemlerine teşvik, terör amaçlı bilgi toplama ve yayma dahil olmak üzere çok çeşitli amaçlarla internetin artan kullanımını yönlendiren stratejik faktörlerden biridir. Birçok faydası aşikâr olmakla birlikte, internet terör örgütleri içinde iletişimi kolaylaştırmak, planlı terör eylemleri hakkında bilgi iletmek ve teröristlere finansman desteği sağlamak için de kullanılabilmektedir (Birleşmiş Milletler Uyuşturucu ve Suç Ofisi, 2012, s. 3-12). Son yıllarda teröristlerin internet kullanımının oluşturduğu tehdidin uluslararası düzeyde tanınmasına rağmen, şu anda özellikle terör eyleminin bu yaygın yönünü ele alan evrensel bir araç bulunmamaktadır. Ayrıca, internet kullanımını içeren terör davalarının soruşturulması ve kovuşturulmasının yasal ve pratik yönleri hakkında uzmanlık eğitimi oldukça sınırlıdır.

Daha önce de ifade edildiği üzere, terör örgütleri interneti fon ve kaynak toplamak için farklı şekillerde kullanabilmektedir. Başlıca yöntemleri doğrudan yardım talep etmek ve e-ticaret sitelerini, çevrimiçi ödeme araçlarını ve hayır kurumlarını istismar etmektir. Doğrudan talep, teröristlerin destekçilerden bağış istemek için web sitelerini, sohbet gruplarını, toplu elektronik postaları ve hedefli iletişimleri kullanması anlamına gelmektedir. Web siteleri, destekçilere kitap, ses ve video kayıtları ve diğer öğeleri sunan çevrimiçi mağazalar olarak da kullanılabilmektedir. Özel web siteleri veya iletişim platformları aracılığıyla sunulan çevrimiçi ödeme olanakları, taraflar arasında elektronik olarak para transferini kolaylaştırmaktadır. Para transferleri genellikle elektronik banka havalesi, kredi kartı, PayPal veya Skype gibi hizmetler aracılığıyla sunulan alternatif ödeme imkanlarıyla yapılmaktadır. Ayrıca, kimlik hırsızlığı, kredi kartı hırsızlığı, elektronik dolandırıcılık, hisse senedi dolandırıcılığı, fikri mülkiyet suçları ve açık artırma dolandırıcılığı gibi dolandırıcılık yollarıyla da çevrimiçi ödeme olanakları istismar edilebilmektedir.

Bununla birlikte, hayır kurumları gibi görünüşte meşru kuruluşlara sağlanan mali destek, yasadışı amaçlar için de yönlendirilebilmektedir. Bazı terör örgütlerinin, çevrimiçi bağış toplamak için hayırsever teşebbüsler kılığında paravan şirketler kurdukları bilinmektedir. Bu kuruluşlar insani amaçları desteklediğini iddia edebilirken, aslında bağışlar terör eylemlerini finanse etmek için kullanılmaktadır. Teröristler, terör örgütlerinin ideolojilerini desteklemek veya militan gruplara maddi destek sağlamak için bir örtü olarak kullandıkları farklı yardım kuruluşlarının yönetimlerine de sızabilmektedir (Conway, 2016, s. 12-14).

3. Bulgular: Terörizmin Finansmanında Kripto Paraların ve Sanal Paraların Rolü

Kripto para birimleri, para birimlerinin oluşturulması ve yönetimi için kriptografi formülünü benimseyen dijital para birimleridir. Kriptografi, düz metni anlaşılmaz alfanümerik metne dönüştürme ve bu işlemi tam tersi şekilde dönüştürme işlemidir. Sadece amaçlananların okuyabilmesi ve işleyebilmesi için verileri belirli bir biçimde depolama ve iletme yöntemidir. Zaman geçtikçe, kripto para birimlerinin sayısı hızla artmakta ve bu da dijital dünyadaki tüm kripto para birimlerini takip etmeyi zorlaştırmaktadır. Şu anda dijital ekonomide 1.500'den fazla kripto para birimi mevcuttur. Kripto para hacimleri her geçen gün yeni rekorlar kırarken, çeşitli terör örgütleri bu kripto para birimlerini, ilgili ülkelerin bankacılık sisteminin gözetim mekanizmasını atlayarak dünya çapındaki terör faaliyetlerini anonim olarak finanse etmek için kullanmaktadır (Majumder, Routh ve Singha, 2019, s. 125).

Sanal para birimleri, bir merkez bankası tarafından çıkarılmayan veya garanti edilmeyen, ödeme aracı olarak hareket edebilen, düzenlenmemiş bir dijital para biçimi olarak tanımlanmaktadır. Sanal para birimleri, ilk olarak çevrimiçi bilgisayar oyun ortamlarında ve sosyal ağlarda para birimleri olarak ortaya çıkmıştır. Daha sonra çevrimdışı veya gerçek hayatta kabul edilen ödeme araçlarına dönüşmüştür. Perakendeciler, restoranlar ve eğlence mekanları ile mal ve hizmetler için ödeme yapmak için sanal para birimlerini kullanmak artık giderek daha fazla mümkün hale gelmektedir. Bu işlemler genellikle herhangi bir ücret veya masraf gerektirmemekte ve bir banka işlemini içermemektedir. Dijital ödeme sisteminde, her iki tarafın da fiziki mevcudiyeti zorunlu olmadığı gibi, fiziksel para birimi de gerekli değildir. Sanal para birimleri, geleneksel para birimleri kullanılarak bir değişim platformunda satın alınabilmektedir. Daha sonra dijital cüzdan olarak bilinen kişiselleştirilmiş bir hesaba aktarılmaktadır. Tüketiciler bu cüzdanı kullanarak sanal para birimlerini kabul etmek isteyen herkese çevrimiçi olarak gönderebilmekte veya bunları Euro, Pound veya Dolar gibi geleneksel bir itibari para birimine geri dönüştürebilmektedir.

Nakit veya diğer dijital işlemlerin yerini almak için şifrelenmiş bir para birimi olan "Bitcoin" adlı dijital dünyadaki ilk ve en popüler kripto para birimi, ilk olarak 2009'da halka açık kaynak kodlu bir yazılım olarak piyasaya sürülmüştür. Önceleri Bitcoin'in yalnızca madenciliği yapılmış; ancak ticareti yapılmamıştır. Fakat 2010 yılında ilk kez 10.000 birim Bitcoin sadece iki pizzayla takas edilmiştir (Russo, 2018). 2011 ve 2012'de diğer birçok kripto para biriminin piyasaya girmesiyle birlikte, dünya genelinde değeri ve popülaritesinde büyük bir artış eğilimi fark edilmiştir. İlk altcoinler (alternatif paralar veya bitcoin dışındaki kripto para birimleri), Litecoin ve Namecoin 2011 yılında piyasaya sürülmüştür. Ardından birçok yeni kripto paranın piyasaya girmesiyle dev bir ekosistem oluşmuştur. Kripto paraların merkezi olmama, anonimlik, eşlerarası olma, yüksek işlem hızı, küresel ve dijital olma gibi özellikleri sayesinde kısa sürede siber suçlarda ve terörizmin finansmanında kullanılması gündeme gelmiştir.

Avrupa Bankacılık Otoritesi (2013), çalınabilecekleri, ödeme araçlarının savunmasız olduğu ve tüketicilerin vergi yükümlülüklerine tâbi kripto paraları elinde bulundurabilecekleri gerekçesiyle kripto para birimlerinin güvensiz olduğu konusunda tüketicilere bir uyarı yayınlamıştır. Aynı kuruluş, Temmuz 2014'te sanal para birimleri hakkında başka bir görüş yayınlayarak, "sanal para birimlerinin yargı sınırlarına uymadığı ve bu nedenle mali yaptırımları ve varlıklara el konulmasını baltalayabileceği; ve piyasa katılımcılarının sağlam kurumsal yönetim düzenlemelerinden yoksun olduğu" uyarısında bulunmuştur (Avrupa Bankacılık Otoritesi, 2014, s. 5).

Türkiye'de ise 16 Nisan 2021 tarihli 31456 sayılı Resmî Gazetede yayımlanan "Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik"le birlikte, "ödemelerde kripto varlıkların kullanılmamasına, ödeme hizmetlerinin sunulmasında ve elektronik para ihracında kripto varlıkların doğrudan veya dolaylı olarak kullanılmamasına ve ödeme ve elektronik para kuruluşlarının kripto varlıklara ilişkin alım satım, saklama, transfer veya ihraç hizmeti sunan platformlara veya bu platformlardan yapılacak fon aktarımlarına aracılık etmemesine" karar verilmiştir. Böylelikle bizzat Türkiye Cumhuriyet Merkez Bankası tarafından, kripto varlıkların ödemelerde kullanılmasının önüne geçilmiştir.

Kripto paralar, uyuşturucu ticareti, insan kaçakçılığı, terörist faaliyetler ve dolandırıcılık gibi yasa dışı faaliyetlerden elde edilen gelirin gerçek niteliğini ve kaynağını kamufle etmekte kolayca kullanılabilmektedir. Bu paralar, ana akım ekonomide kullanılabilecek şekilde kolayca temiz paraya dönüştürülebilmektedir. Ayrıca proxy sunucuların ve olağan dışı yazılımların kullanılması, yasadışı kripto para birimi işlemleri yapan kullanıcıların internet protokol (IP) adresinin takip edilmesini oldukça zorlaştırmıştır (Majumder ve ark., 2019, s. 132). Kara para aklama için kripto para birimini seçmenin başlıca nedeni, finansal işlemde yer alan kişinin gerçek kimliğini gizlemeye yardımcı olan anonimliğidir. Piyasadaki mevcut kripto para birimlerinden Monero ve Zcash gibi birkaç para birimi tamamen özerktir ve bir kişi veya kuruluşla ilişkilendirilememektedir. ABD Adalet Bakanlığı Uyuşturucuyla Mücadele İdaresi raporuna göre Bitcoin, uluslararası suç örgütlerinin uluslararası yasadışı para transferine yardımcı olması ve kara para aklamada kullanılması nedeniyle bir tehdit olarak ortaya çıkmıştır. Ancak bu kanıtlara rağmen, her tür kripto para biriminin kullanımını sadece birkaç ülke kısıtlamaktadır (De, 2017).

Uluslararası düzeyde, kripto para birimlerine yönelik düzenleyici adımlar, ilgili uluslararası kuruluşların belirli alanlarda raporlar, kılavuzlar ve el kitapları yayınlamasından oluşmaktadır. Bu kapsamda Uluslararası Para Fonu (IMF), G20, Ekonomik Kalkınma ve İşbirliği Örgütü (OECD), Malî Eylem Görev Gücü (FATF) ve Avrupa Birliği (AB) gibi kuruluşlar çeşitli yayınlarla kripto para konusunda düzenleyici bir çerçeve oluşturmaya çalışmaktadır. Örneğin, başlangıçta kripto paraların sistemik bir risk oluşturmadığını belirten IMF, 2018'de merkez bankalarına gönderdiği uyarıcı bir notla, kripto para birimlerinin kara para aklama ve terörizmin finansmanı gibi konularda kullanılmasıyla ilgili endişelerini dile getirmiştir (He, 2018, s. 16). Benzer şekilde, 2018'de Arjantin'deki G20 toplantısında ve Davos'taki 2018 Dünya Ekonomik Forumu sırasında kripto para birimleriyle ilgili düzenlemeye uyumlu bir uluslararası yaklaşım için çağrılar yapılmıştır. OECD, kripto para birimlerinin küresel düzenlemesinde koordine edici bir rol oynama niyetini ifade etmiştir. Temel hedefi, kara para aklama, terörizm finansmanı ve diğer ilgili tehditlerle mücadeleyle alakalı standartları belirlemek olan FATF, sanal para birimlerine yönelik risk temelli bir yaklaşım hakkında rehberlik sağlayan bir rapor yayınlamıştır (Motsi-Omoijiade, 2022, s. 30-40).

Kripto para birimlerinin ulusal düzeyde düzenlenmesi ise ülkeden ülkeye farklılık göstermektedir. Bu konuda bazı ülkeler hiçbir düzenleme yapmazken, bazı ülkeler hafif düzenlemeler yapmakta; bazıları ise oldukça sıkı ve kısıtlayıcı düzenlemeler ortaya koymaktadır. Dolayısıyla ülkelerin kripto paraya yaklaşımıyla ilgili çeşitli kategorizasyonlar yapılmaktadır. Örneğin, Bloomberg (2018) yayınladığı çalışmada, dünyanın kripto para ticaretinin çoğunun teknoloji meraklısı Asya'da gerçekleştiğini belirterek ülkeleri tek tek incelemektedir. Japonya'nın dijital varlık alışverişi için bir lisanslama sistemi getirdikten sonra baskın bir rol oynadığını belirtmektedir. Singapur'un kripto paralara yumuşak bir yaklaşım sergilediği, Tayvan'ın bekle-gör politikası izlediği ve bir zamanlar kripto para ticareti için küresel merkez olan Çin'in şimdi kripto paraları çökertmede dünyaya öncülük ettiği ifade edilmektedir. Güney Kore kripto para ticaretini serbest bırakırken, Hindistan'ın dijital para birimlerini yasal ödeme aracı olarak görmediği ve kullanımlarını engellemek için önlemler aldığı vurgulanmaktadır. Diğer bütün kıtalarda da buna benzer ülke bazlı farklılıklar görülmektedir.

Siber suçun önemli bir unsuru, Dark Web'de kaçak mal ve hizmet satın almak ve satmak için Bitcoin gibi kripto para birimlerinin kullanılmasıdır. Dark Web, sağladığı coğrafi kapsam, hız ve anonimlik derecesi göz önüne alındığında teröristlerin ilgisini çekmektedir. Ancak Dark Web risksiz değildir. Kripto para birimleri, kripto para biriminin gönderildiği kaynak elektronik cüzdanı izlemek için kullanılabilecek blok zincirlere eklendiklerinden, tam bir anonimlik sağlamaktan ziyade daha fazla anonimlik sağlamaktadır (Carroll ve Windle, 2018, s. 288). Her ne kadar kripto para birimlerini takip etmek zor olsa da güvenlik güçleri, kripto para kullanıcılarının davranışlarının ve rutin finansal faaliyetlerinin bir resmini oluşturmak için bütün verilerden istifade etmektedir. Diğer taraftan, kripto para birimleri emekleme dönemindedir ve gelecekte daha güvenli hale gelebilir ve izlenmesi daha da zorlaşabilir. Bu da terörist finansörlerin yakalanma riskini daha da azaltacaktır.

Günümüzde sanal dünyalar terörizmin finansmanının gerçekleştirilebileceği diğer teknolojik mecralardır. Castronova'ya göre (2001), sanal dünya, üç tanımlayıcı özelliği olan bir bilgisayar programıdır: Etkileşim, fiziksellik ve kalıcılık. Bell (2008, s. 2) ise sanal dünyaları "uzayda avatarlar tarafından temsil edilen çok sayıda katılımcı tarafından aynı anda deneyimlenebilen kalıcı bir sanal ortamın uzamsal tabanlı bir tasviri" olarak tanımlamaktadır. Bu ortamlar, insanların gerçek veya hayali yaşamları simüle ettiği bilgisayar tabanlı platformlardır. Bu sanal dünyalar içinde ekonomiler, toplumlar ve kişisel ilişkiler gelişmektedir. Bu bağlamda sanal dünyalar, kara para aklamanın ve terörizmin finansmanının gerçekleşmesi için olası bir yer olarak ortaya çıkmaktadır. Şunu vurgulamak gerekir ki bu durum, dijital veya kripto para birimlerini kara para aklama aracı olarak kullanmakla aynı şey değildir. Çünkü kripto para kullanılması durumunda para birimi sanal bir para birimi olsa bile olayın sonuçları gerçek dünyada gerçekleşmektedir. Sanal ortam suç faaliyetinin mekânı olarak kullanılırken; sanal para ile para aklama suç gelirlerini gizlemek için interneti veya diğer elektronik ödeme sistemlerini kullanma anlamına gelmektedir (Chambers-Jones, 2018, s. 166).

Avrupa Bankacılık Otoritesi (2014, s. 11), sanal para birimlerini "bir merkez bankası veya kamu otoritesi tarafından çıkarılmayan veya bir itibari para birimine zorunlu olarak bağlı olmayan, ancak gerçek veya tüzel kişiler tarafından bir değer olarak kullanılan, elektronik olarak transfer edilebilen, saklanabilen veya alınıp satılabilen dijital bir değer temsili" olarak tanımlamaktadır. Bu nedenle, Second

Life platformundaki Linden Doları gibi sanal dünyalarda kullanılan sanal para birimleri, Bitcoin gibi diğer dijital para birimleriyle aynı kabul edilmektedir. İki tür sanal para vardır: Tanımlanmış sanal para ve anonim sanal para. Tanımlanan sanal para, birine ait olarak tanımlanabilmektedir ve bir bankacılık kurumundan para çekme işlemiyle bağlantılıdır. Başka bir deyişle, izlenebilmektedir. Anonim sanal para ise izlenememektedir. Hesaptan çekildiğinde, fark edilebilir bir iz bırakmamaktadır. Daha sonra bu parayla gerçekleştirilebilecek çok sayıda suç faaliyeti bulunmaktadır. Terörizmin finansmanı bunlardan yalnızca bir tanesidir.

Second Life, kendine özgü bir kültür ve ekonomi geliştirmiş, 3 boyutlu, sürükleyici, platform tabanlı bir sanal çevre oyunu dünyasıdır. Ekonomisi, platformun sahibi olan teknik geliştirme şirketi Linden Labs'ın adını taşıyan dünya para birimi Linden Dolarına dayanmaktadır. Bu sanal dünya biçimi oyuncular arasında popülerdir. Aynı zamanda çevreyi öğrenme ve eğitim için bir platform olarak kullanan akademisyenler ve sağlık uzmanları arasında da oldukça ünlüdür. Bu sanal platformlar, bütün bunların yanında suçlular tarafından yasa dışı faaliyet yürütmenin bir aracı olarak da kullanılabilmektedir (Chambers-Jones, 2012).

Interpol, sanal paranın yasadışı kullanımı kapsamında şu faaliyetlerden bahsetmektedir: Sanal paranın yetkisiz üretilmesi, aktarılması veya geri alınması; sistem içindeki fonların niteliğini yasa dışı olarak değiştirmek için kullanılan bilgisayar sistemlerine kriminal erişim; sanal para sistemi üzerinde sanal para değer kaybına veya fonksiyon kaybına yol açan sanal para sistemlerine yönelik kriminal saldırılar; sanal para sistemlerinin mali suçlar için cezai olarak kötüye kullanılması veya diğer mali sistemleri yıkmak veya kötüye kullanmak için bir araç olarak kullanılması. Bütün bunların yanında, suçluların geçmişte para toplamanın failler için sorunlu olduğu şantaj, adam kaçırma veya gasp gibi vakalarda yakalanma olasılığını azaltmak için sanal para talep etmesi, özellikle anonim sanal para açısından önem taşımaktadır (Kerr, 2003, s. 372–373).

4. Sonuç

Teröristler, militan toplamak ve desteklemek, lojistik merkezler kurmak ve yönetmek ve operasyonları yürütmek için finansmana ihtiyaç duymaktadır. Bu kapsamda, terörist gruplar, faaliyetlerini finanse etmek için interneti ve sanal dünyayı yaygın bir şekilde kullanmaktadır. Doğrudan internet üzerinden bağış toplayarak, elektronik ticaret yaparak, çevrimiçi kumar faaliyetleri yürüterek, online ödeme sistemlerini manipüle ederek, dijital para çalarak, Dark Web'de uyuşturucu ve yasa dışı ürünler satarak veya hayır kurumu benzeri yapıları istismar ederek önemli finansal kaynaklar elde etmektedir. İnternet ve mobil teknolojilerin sağladığı teknolojik imkanlar terör örgütlerinin kara para aklamasına da yardım etmektedir. Bitcoin benzeri dijital para birimleri veya Linden Doları benzeri sanal paralar, bu örgütlerin gizlice para transfer etmesine olanak tanımaktadır.

Finansman, geniş bölgeleri kontrol eden büyük terör örgütlerinden küçük terör hücrelerine kadar tüm teröristler için önemlidir. Önemli bir varsayım, finansal verilerin özellikle değerli olduğu fikridir; çünkü bu anlayışa göre para izleri asla yalan söylememektedir. Özellikle 11 Eylül 2001'den bu yana, şüpheli ve terör paralarının takibi önemli bir politika endişesi olarak ortaya çıkmıştır. Finansal işlemler, şüpheli işlemleri işaretlemek ve terörist faaliyetleri hazırlık aşamasında tespit etmek için analiz edilmekte, araştırılmakta, raporlanmakta ve dağıtılmaktadır. Finansal işlemlerin değerli istihbarat sağladığı; özellikle de terörist faaliyetin ve dahil olan oyuncuların saptanması açısından değerli olduğu yaygın bir şekilde kabul görmektedir (Goede, 2018, s. 756).

Teröristler, finansman toplama ve taşıma da dahil olmak üzere operasyonlarının tüm yönleri için interneti kullanmaya devam edeceklerdir. Bu eğilimin internetin kapsamı ve ölçeği genişledikçe ve diğer ilgili teknolojik gelişmelerle birlikte artması muhtemeldir. Bu noktada, internetin terörle mücadelede ciddi güvenlik açıkları oluşturduğu ve bu büyüyen tehdide karşı önlem alınması gerektiği konusunda hükümetler arasında yaygın bir fikir birliği olduğu söylenebilir. Ancak, atılması gereken adımlar konusunda çok daha az uzlaşı vardır. Her ülke bu alanda yeterli önlemleri alamamakta ve siber alandaki terörizm finansmanıyla ilgili uluslararası iş birliği yetersiz kalmaktadır. Jacobson'un (2010, s. 359-360) da vurguladığı üzere, bu durumun çeşitli sebepleri vardır.

Birincisi, birçok ülke çevrimiçi terör faaliyetlerini araştırmak için gerekli teknik yeteneklerden yoksundur. İkinci olarak, hükümetlerin internetle ilgili faaliyetleri engellemede ne kadar ileri gitmesi gerektiği konusunda hala bir tartışma vardır. Bazı hükümetler, bu adımların atılmasının ifade özgürlüğü

hakkını kısıtlayacağından endişe duymaktadır. Üçüncüsü, bu alandaki yasalar teknolojik değişimlere ayak uyduramamış durumdadır ve ilerlemek için hangi değişikliklerin yapılması gerektiği konusunda bir uzlaşı yoktur. Dördüncüsü, bazı ülkeler bu alanı yönetecek bir uluslararası hukuk aracının veya antlaşmanın kurulmasından yana olsalar da tüm hükümetler bunu ileriye dönük gerekli veya yararlı bir adım olarak görmemektedir. Ve son olarak, ülkeler harekete geçmeye karar verdiklerinde bile, terör örgütleri hemen karşı atağa geçebilmektedir. Ortaya çıkan yeni teknolojiler, teröristlerin çabalarını kolaylaştırmakta ve hükümetin izleme gayretlerini zorlaştırmaktadır.

Dolayısıyla, siber dünyadaki kripto para birimleri gibi gelişmeler terörizmin finansmanı konusunda terör örgütlerine fırsatlar sunmaktadır. Aynı teknolojiler güvenlik güçlerinin suç ve suçluları takibi için de bazı araçları mümkün kılmaktadır. İyi ile kötü arasındaki bu yarış önümüzdeki süreçte de hız kesmeden devam edecektir. Hükümetler, terörist suç girişimlerini kapsamlı bir tehdit olarak incelemek zorundadır. Suç eylemlerinin kovuşturulması aşırılık yanlısı davranışlardan çok daha kolay olduğundan, her ülkede bu suç faaliyetlerine karışan teröristleri durdurmak için entegre bir yaklaşım başlatılmalıdır. İnternet çağında bu fiziksel sınırların oluşturduğu boşlukları kapatmak için hükümetler ulusal sınırların ötesinde gelişmiş iş birliği ve bilgi paylaşımında bulunmalıdır. Yenilikleri en iyi takip eden ve hatta yönlendirebilen taraf, en azından bir süreliğine, yarışın galibi olacaktır.

Kaynaklar

Avrupa Bankacılık Otoritesi. (2013, 12 Aralık). *EBA Warns Consumers on Virtual Currencies*. https://www.eba.europa.eu/eba-warns-consumers-on-virtual-currencies

Avrupa Bankacılık Otoritesi. (2014, 4 Temmuz). *Opinion on Virtual Currencies*, EBA/Op/2014/08.

Bantekas, I. (2003). The International Law of Terrorist Financing. *The American Journal of International Law*, 97(2), 315-333.

Bell, M. (2008). Towards a Definition of Virtual Worlds. *Journal of Virtual World Research*, 1(1), 2-5. https://doi.org/10.4101/jvwr.v1i1.283

Biersteker, T. J. & Eckert, S. E. (2008). *Countering the Financing of Terrorism*. London: Routledge.

Birleşmiş Milletler. (1999). *International Convention for the Suppression of the Financing of Terrorism*.

Birleşmiş Milletler Uyuşturucu ve Suç Ofisi. (2012). *The Use of the Internet for Terrorist Purposes*. New York.

Bloomberg. (2018, 26 March). What the World's Governments Are Saying About Cryptocurrencies, https://www.bloomberg.com/news/articles/2018-03-26/what-the-world-s-governments-are-saying-about-cryptocurrencies

Carroll, P. & 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. https://doi.org/10.1080/18335330.2018.1506149

Castronova, E. (2001). *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier*, 618 CESifo Working Papers.

Chambers-Jones, C. (2012). *Virtual Economies and Financial Crime: Money Laundering in Cyberspace*. Surrey: Edward Elgar Publishing.

Chambers-Jones, C. (2018). Money Laundering in a Virtual World. In C. King, C. Walker & Jimmy Gurulé (Eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 165-182). Palgrave Macmillan.

Conway, M. (2006). Terrorist 'Use' of the Internet and Fighting Back. *Information & Security*, 19, 9-30. http://dx.doi.org/10.11610/isij.1901

De, N. (2017, 25 October). DEA Report: Bitcoin Used for Trade-Based Money Laundering. *Coindesk*, https://www.coindesk.com/markets/2017/10/25/dea-report-bitcoin-used-for-trade-based-money-laundering/

Dilipraj, E. (2019). *Cyber Enigma: Unravelling the Terror in the Cyber World*. London: Routledge.

Europol. (2022). *European Union Terrorism Situation and Trends Report 2022*. https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

FBI. (2022). *Internet Crime Report 2021*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Freeman, M. (2011). The Sources of Terrorist Financing: Theory and Typology. *Studies in Conflict & Terrorism*, 34(6), 461-475. http://dx.doi.org/10.1080/1057610X.2011.571193

Goede, M. (2018). Counter-Terrorism Financing Assemblages After 9/11. In C. King, C. Walker & Jimmy Gurulé (Eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 755-779). Palgrave Macmillan.

He, D. (2018). Monetary Policy in the Digital Age. *Finance and Development*, 13-16, https://www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.pdf

Ilbiz, E. (2019). The Uberization of the United Nations' Regime to Prevent the Online Financing of Terrorism: Tackling the Problem of Obfuscation in Virtual Currencies. *Journal of Cyber Policy*, https://doi.org/10.1080/23738871.2019.1666892

Jacobson, Michael. (2010). Terrorist Financing and the Internet, *Studies in Conflict & Terrorism*, 33(4), 353-363. http://dx.doi.org/10.1080/10576101003587184

Kerr, O. (2003). The Problem of Perspective in Internet Law. *Georgetown Law Journal*, 91(2), 357-405. http://dx.doi.org/10.2139/ssrn.310020

Majumder, A., Routh, M. & Singha, D. (2019). A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing. In *The Impact of Global Terrorism on Economic and Political Development* (pp. 125-138).

Morgan, S. (2020, 13 November). Cybercrime To Cost The World $10.5 Trillion Annually By 2025 [Web blog post]. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Motsi-Omoijiade, I. D. (2022). *Cryptocurrency Regulation A Reflexive Law Approach*. London: Routledge.

Resmî Gazete. (2013, 16 Şubat). Sayı: 28561. *Terörizmin Finansmanının Önlenmesi Hakkında Kanun*. Kanun No. 6415.

Resmî Gazete. (2021, 16 Nisan). Sayı: 31456. *Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik*.

Russo, C. (2018, 26 Şubat). Crypto legend who brought pizza with 10000 bitcoin is back at it. Retrieved from https://www.bloomberg.com/news/articles/2018-02-26/crypto-legend-who-bought-pizza-with-10-000-bitcoin-is-back-at-it.

Schott, P. A. (2006). *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: Second Edition and Supplement on Special Recommendation IX*. Washington: World Bank.

Thachuk, K. L. & Lal, R. (2018). *Terrorist Criminal Enterprises: Financing Terrorism through Organized Crime*. Santa Barbara: Praeger.

Wall, D. S. (2005). The Internet as a Conduit for Criminals. In A. Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 77–98). Thousand Oaks: Sage.

WeAreSocial & Hootsuiye. (2020). *Digital 2020: Global Digital Overview*. Retrieved from https://wearesocial.com/digital-2020

Weimann, G. (2006). Virtual Disputes: The Use of the Internet for Terrorist Debates. *Studies in Conflict & Terrorism*, 29, 623-639. https://doi.org/10.1080/10576100600912258

Yanarışık, O. (2020). İç Güvenlik ve Siber Güvenlik. İ. İrdem (Ed.), *İç Güvenlik Yönetimi ve Polislik* içinde (s. 303-327). Ankara: Polis Akademisi Yayınları.

Research Article

Terörizmin Finansmanında Siber Tehditler ve Kripto Paraların Rolü

Cyber Threats and the Role of Crypto Currencies in the Financing of Terrorism

Oğuzhan Yanarışık
Dr. Öğretim Üyesi, Polis Akademisi
Güvenlik Bilimleri Enstitüsü
yanarisik@gmail.com
https://orcid.org/0000-0003-3442-4779

Extensive Summary

Terrorist activities take place in many different forms, from individual acts to the planned activities of organized groups. Therefore, the forms of financing of terrorism change accordingly. Terrorist organizations need significant funds both for the actual realization of terrorist acts and to maintain the functioning of the organization, to provide its basic technical requirements and to cover the costs related to the spread of their ideology. Terrorist groups need money to survive and carry out terrorist acts. Financing of terrorism covers the tools and methods used by terrorist organizations to finance their activities. This money can come from sources that are perceived to be legitimate, such as profits from legitimate-looking businesses and charities. In addition, terrorist groups can also finance illegal activities such as arms, drugs or human trafficking, illegal commodity trade (oil, coal, diamonds, gold and narcotics), or kidnapping for ransom. Recently, the role of the cyber world and cryptocurrencies in the financing of terrorism has been increasing.

The cyber world provides a virtual bridge between borders, allowing crime to be carried out on a larger scale, faster and with greater potential for return. As a result, the extent of cyber victimization and online sales of contraband is constantly increasing. Cyberspace can also provide a suitable basis for real-life illegal activities such as credit card fraud, drug dealing, extortion, illegal arms and ammunition exchange, identity theft, money laundering and online checking of vulnerable people for exploitation in criminal activities.

Cryptocurrencies can support illegal activities and terrorism, since they contain no information about the origin of the money and can be converted into cash and traded by the owner when necessary. Cryptocurrencies operate on digital platforms that can be manipulated by smart hackers and enable cyber-attacks. Recently, terrorism has been growing simultaneously with cryptocurrencies. With the development of technology, the cyber world has become a very serious channel in the financing of terrorism. In other words, terrorist organizations and their supporters are increasingly using the internet to finance terrorist acts. The ways in which terrorists use the internet to raise funds and resources can be classified into four general categories: soliciting direct funding from their supporters, exploiting e-commerce sites, exploiting online payment tools, and exploiting charities.

Cryptocurrencies can easily be used to camouflage the true nature and source of income from illegal activities such as drug dealing, human trafficking, terrorist activities and fraud. These coins can be easily converted into clean money that can be used in the mainstream economy. In addition, the use of proxy servers and unusual software has made it very difficult to trace the internet protocol (IP) address of users who engage in illegal cryptocurrency transactions. The primary reason for choosing cryptocurrency for money laundering is its anonymity, which helps hide the true identity of the person involved in the financial transaction. Of the existing cryptocurrencies in the market, a few currencies such as Monero and Zcash are completely autonomous and cannot be associated with a person or organization.

According to the US Department of Justice Drug Enforcement Administration report, Bitcoin has emerged as a threat because it helps international criminal organizations to transfer money internationally and is used in money laundering. But despite this evidence, only a few countries restrict the use of any type of cryptocurrency.

Today, virtual worlds are other technological channels where the financing of terrorism can be realized. These environments are computer-based platforms where people simulate real or imagined lives. Within these virtual worlds, economies, societies and personal relationships develop. In this context, virtual worlds are emerging as a possible place for money laundering and terrorist financing to take place. The European Banking Authority defines virtual currencies as a digital currency that is not issued by a central bank or public authority or is not necessarily tied to a Fiat Currency, but can be transferred, stored or traded electronically, used as a value by natural or legal persons. value representation. Therefore, virtual currencies used in virtual worlds, such as the Linden Dollar on the Second Life platform, are considered the same as other digital currencies such as Bitcoin.

There is evidence that cryptocurrencies are used by terrorist organizations to raise money or buy goods. However, this evidence tends to be generally unconfirmed and anecdotal. Moreover, the cases cited are relatively few and involve relatively small amounts of income. Because it is very difficult to trace cryptocurrencies and associate them with terrorist activities. However, the internet has changed the organizational nature of criminal activity by giving "lone (single) criminals..." the ability to perform incredibly complex and far-reaching tasks that can be repeated countless times on a global scale. Therefore, we are likely to see the emergence of what might be termed lone wolf cyber-financiers: individuals not affiliated with any physical terrorist cell can raise money through criminal activity to aid terrorism.

Terrorists will continue to use the internet for all aspects of their operations, including collecting and transporting funds. This trend is likely to increase as the scope and scale of the Internet expands and along with other related technological developments. At this point, it can be said that there is a widespread consensus among governments that the internet creates serious security gaps in the fight against terrorism and that measures should be taken against this growing threat. However, there is much less consensus on the steps to be taken. Not every country can take adequate measures in this area, and international cooperation in cyber terrorism financing remains insufficient. There are various reasons for this situation:

First, many countries lack the necessary technical capabilities to investigate terrorist activities online. Second, there is still debate about how far governments should go in blocking internet-related activities. Some governments are concerned that taking these steps will restrict the right to freedom of expression. Third, laws in this area have not kept pace with technological changes, and there is no consensus on what changes need to be made to move forward. Fourth, although some countries favor the establishment of an instrument of international law or treaty to govern this area, not all governments see it as a necessary or beneficial step forward. And finally, even when countries decide to take action, terrorist organizations can immediately counterattack. Emerging new technologies facilitate terrorist efforts and complicate government surveillance efforts.

Therefore, developments such as cryptocurrencies in the cyber world offer opportunities to terrorist organizations in the financing of terrorism. The same technologies also enable some tools for security forces to track crime and criminals. This race between good and evil will continue unabated in the upcoming period. The party that follows and even directs the innovations best will be the winner of the race, at least for a while.