SİBER TERÖRİZM VE IŞİD-BITCOIN İLİŞKİSİ

"ABD hegomanyası altındaki başta bölge ülkeleri, NATO ve Avrupa terörle mücadele şekillerini ABD'ni önceleyen politikalara doğru evirmişlerdir. Dolayısıyla da ulusların terörizm ile mücadele ve güvenlik politikaları değişime uğramıştır."

Emine Çelik
Doktora Öğrencisi, Necmettin Erbakan Üniversitesi

11 Eylül 2001'de ABD'de gerçekleştirilen terör saldırıları terörizmin tüm dünyada yeniden tartışılmasına zemin hazırlamıştır. Saldırı sonrası dönemin ABD başkanı George W. Bush'un 20 Eylül'de Kongre'deki konuşmasında sarf ettiği "*Tüm bölgelerde tüm ülkeler, şimdi bir karar vermelidir. Ya bizimlesiniz ya da teröristlerle*" ifadesinin akabinde ABD'nin terörizm ile mücadele adı altında Afganistan ve Irak'a orantısız müdahalelerde bulunmuştur. Bu süreçte ulusların tepkilerine rağmen, Bush'un yapmış olduğu açıklama sonrasında özellikle terörle mücadele başlığı altında başta Afganistan ve Irak müdahalesi bölge ülkelerinin tepkisine neden olmuştur. ABD hegomanyası altındaki başta bölge ülkeleri, NATO ve Avrupa terörle mücadele şekillerini ABD'ni önceleyen politikalara doğru evirmişlerdir. Dolayısıyla da ulusların terörizm ile mücadele ve güvenlik politikaları değişime uğramıştır. 11 Eylül sonrasında değişen terörizm algısıyla ABD'nin Ortadoğu'ya müdahalesi, kırılgan olan bölgenin daha da istikrarsızlaşmasına neden olmuş, akabinde 2010 yılında Ortadoğu'nun birçok ülkesinde ortaya çıkan Arap Baharı protestoları ile de Irak, Suriye, Libya, Yemen gibi bölge ülkeleri kaosa sürüklenmiştir. Ortadoğu bölgesinde istikrarın ve devlet mekanizmasının işlevselliğini yitirmesi, özellikle Irak ve Suriye'de devlet dışı silahlı aktörlerin faaliyet alanlarını giderek genişletmelerine neden olmuştur. Dönemin şartlarına ayak uydurarak bilgi iletişim teknolojilerini ve interneti aktif olarak kullanmaları devlet dışı aktörlerin yeni bir alan-

da daha faaliyet göstermelerine kapı aralamıştır. Özellikle 11 Eylül sonrasında ulusların terörizm ile mücadele konusunda artan baskıları neticesinde teknolojik gelişmelere de aktif bir şekilde adapte olan devlet dışı aktörlerin bu alanında aktifleşmeleri de terörizm kavramının yeni bir boyuta evirilmesine kapı aralamıştır.

Günümüzde siber alandaki saldırıların -StuxNet ve Suud Aramco saldırıları gibi fiziksel dünyaya taşınması ulusların güvenlik endişelerine arttırmıştır. StuxNet saldırısının İsrail ve ABD ortaklığında, Aramco saldırısının ise İran tarafından gerçekleştirildiği uluslararası hukuk bağlamında ispat edilememiştir. Söz konusu saldırıların hukuki bakımdan isnat edileceği bir failin ya da faillerin bulunamaması, saldırının kaynağının tespit edilememesinden yani saldırılarının anonimlik esaslı olmasından kaynaklanmaktadır.

Devlet Dışı Silahlı Aktörler ve Siber Alan

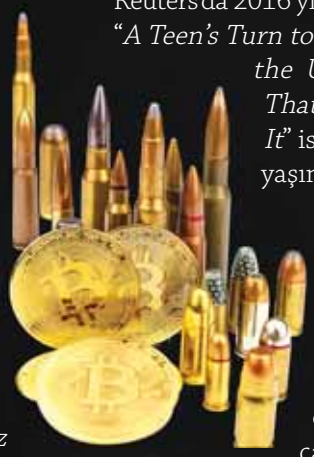
İnternetin ve ona bağlı teknolojinin hızla gelişmesi, iletişim döneminde devrim sayılabilecek YouTube, Twitter, Instagram, Facebook gibi sosyal ağların ortaya çıkışı terör örgütlerinin propaganda, militan devşirme, finansal kaynak sağlama gibi konularda yeni faaliyet alanları oluşturmalarını sağlamıştır. Bu bağlamda siber terörizm kavramı popülerlik kazanmaya başlamış ve yeni bir terörizm alanı olarak ortaya çıkmıştır. Kısa tarihsel arka planına bakıldığında siber terörizmin kökenleri 90'lı yıllara, internetin ortaya çıkışına kadar indirgemek mümkündür. Nitekim ilk dönem gerçekleştirilen siber terörizm eylemlerinin hackerlar tarafından başka bilgisayarlara, sistemlere zarar vermek üzere kurgulandığı bilinmektedir. Dolayısıyla da saldırıların sanal dünyada gerçekleştiği ve fiziksel dünyada zarar vermenin söz konusu olmadığı bilinmektedir. Günümüzde ise siber alandaki saldırıların –StuxNet ve Suud Aramco saldırıları gibi fiziksel dünyaya taşınması ulusların güvenlik endişelerine arttırmıştır. StuxNet saldırısının İsrail ve ABD ortaklığında, Aramco saldırısının ise İran tarafından gerçekleştirildiği uluslararası hukuk bağlamında ispat edilememiştir. Söz konusu saldırıların hukuki bakımdan isnat edileceği bir failin ya da faillerin bulunamaması, saldırının kaynağının tespit edilememesinden yani saldırılarının anonimlik esaslı olmasından kaynaklanmaktadır. Tam da bu noktada devlet dışı silahlı aktörlerin siber alanda anonimlik perdesi arkasında faaliyetlerini artırmaları tüm dünya tarafından endişe ile takip edilmektedir.

Devlet dışı silahlı aktörler arasında bu alanda şüphesiz en dikkat çeken aktör IŞİD olmuş ve IŞİD'in siber alanı aktif bir şekilde kullanması, internet üzerinden militan devşirme yöntemleri ve propaganda şekilleri siber terörizminin boyutlarını gözler önüne sermiştir. Ortaya çıktığı ilk dönemlerde popülerliğini arttırmak adına gerçekleştirdiği sansasyonel eylemleri YouTube üzerinden dünyaya servis etmesi ve sosyal ağlarda, özellikle Facebook ve Twitter'da özendirici içerikler kullanarak yayınlar yapması da, örgütün dünyanın her yerinden militan devşirmesini sağlamıştır. Uluslararası arenada IŞİD ile mücadele kapsamında örgütün sosyal ağlardaki hesapları kapatılmış, militan devşirmesi ve propaganda yapması engellenmeye çalışılmıştır. Aynı zamanda IŞİD'i ortadan kaldırmak amacıyla hem koalisyon ülkeleri tarafından hem de Türkiye'nin Fırat Kalkanı Harekatı gibi askeri operasyonlar düzenlenmiş, örgüt Suriye ve Irak'ta alan hakimiyetini kaybetmeye başlamıştır. Bununla birlikte, örgütün siber alandaki varlığı ise öne çıkan araştırma konularından biri haline gelmiştir.

IŞİD ve Bitcoin İlişkisi

Rand Enstitüsü tarafından yayınlanan *"Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats"* isimli raporda IŞİD'in klasik devlet yapısına sahip olmamasından dolayı uluslar tarafından uygulanan ablukaya ve en önemli gelir kaynakları olarak nitelendirilen petrol piyasalarına erişimlerinin engellenmesinin finansal açıdan örgütün kıskaca alınmasından söz edilmiştir. Ayrıca raporda IŞİD'in uluslararası banka sisteminden de izole edilmesi, ABD tarafından mevcut sistem içerisindeki nakit rezervlerine yönelik hamleler neticesinde de örgütün nakit paraya daha çok bağımlı hale geldiği ifade edilmiştir. Bu bağ-

lamda da örgüt kendisine yeni bir para akış trafiği elde etmek adına özellikle ABD, İngiltere gibi ülkelerden kendi saflarına kattığı bilgisayar mühendisi, hacker vb. militanlar ile siber alana yönelmiştir. Hızla siber alana adapte olan örgüt fiziksel dünyanın aksine siber alanda faaliyet alanını genişletmiştir. Siber alanda da yüzey internetinde çeşitli engellemelere takılan örgüt yüzey internetinden daha geniş ve TOR, I2P gibi özel yazılımsal araçlarla ulaşılabilen, internetin yer altı katmanı olarak ifade edilen Dark Web'de faaliyetlerini sürdürmeye başlamıştır. Silah ve ekipman temini, silah kullanımı, militanların eğitimi ve sempatizanlara yönelik propagandalar IŞİD'in Dark Web'deki faaliyetlerinden bazılardır. Ayrıca kripto para birimleri –özellikle Bitcoin- ile militanlarından ve sempatizanlarından bağış topladıkları, terör eylemlerini de finanse ettikleri bilinmekte ve her geçen gün iletişim kanalı olarak sınıflandırdıkları birimleri siber alanda güçlenmektedir. Bu durum ile ilgili endişesini İngiltere "*Intelligence and Security Committee of Parliament: Annual Report 2016-2017*" raporunda "*IŞİD interneti propaganda amaçlı, aynı zamanda radikalleşme ve operasyonel planlama için kullanıyor. Altyapımıza siber saldırı ile saldırarak insanları öldürmek için henüz interneti kullanmadılar. Henüz bu yeteneğe sahip değiller. Ama istediklerini ve inşa etmek için ellerinden geleni yaptıklarını biliyoruz*" şeklinde ifade etmiştir. Nitekim bu endişelerin yersiz olmadığı IŞİD militanı Ebu Mustafa'nın Ocak 2015'de Dark Web üzerindeki bir siteden İŞID militanlarına ve sempatizanlarına çağrıda bulunmuş ve 1.000 dolar değerinde Bitcoin toplamasıyla ortaya çıkmıştır.



> **2014 yılında Twitter üzerinden IŞİD'e Bitcoin ile nasıl finansal destek sağlanacağına dair mesajlar yayınlamaya başlayan Ali Şukri Amin Twitter mesajları üzerinden, IŞİD'e finansal yardım, IŞİD sempatizanlarının Suriye'ye seyahat etmelerinde yardımcı olmak ile suçlanarak 11 yıl hapse mahkum edilmiştir.**

Reuters'da 2016 yılında yayınlanan "*A Teen's Turn to Radicalism and the U.S. Safety Net That Failed to Stop It*" isimli haberde 17 yaşındaki IŞİD sempatizanı Ali Şukri Amin 2014 yılında Twitter üzerinden IŞİD'e Bitcoin ile nasıl finansal destek sağlanacağına dair mesajlar yayınlamaya başladığı belirtilmiştir. Ali Şukri Amin Twitter üzerinden yayınladığı mesajlar, IŞİD'e finansal yardım, IŞİD sempatizanlarının Suriye'ye seyahat etmelerinde yardımcı olmak ile suçlanarak 11 yıl hapse mahkum edilmiştir. Suçlandığı birçok konuda FBI ile anlaşma yapan Ali Şukri Amin ve IŞİD'in kazancı ise tweetleri ile birçok İŞID sempatizanına kripto paralar üzerinden örgüte nasıl fon sağlanacağına dair bilgiler vermesi olmuştur. The Telegraphy'de Aralık 2017 yılında yer alan "N*ew York Woman Charged with Sending $85.000 in Bitcoin to Support Isil*" isimli haberde 27 yaşındaki laboratuar teknisyeni Pakistan doğumlu ABD vatandaşı olan Zoobia Shahnaz 2015 yılından itibaren IŞİD'e katılmayla ilgili internet üzerinden aramalar yaptığı, Ocak 2016'da Ürdün'de bulunan ve IŞİD'in etki alanında olan Zataari mülteci kampında 2 hafta gönüllü olarak çalıştığı belirtilmiştir. Bu süreçte radikalleştiği düşünülen Shahnaz banka kredisi ve bir düzine kredi kartı ile Bitcoin alarak İŞID'e finansman sağlamıştır. Forbes'da yayınlanan "*How Criminals and Terrorists Use Crytptocurrency: And How To Stop It*" isimli bir başka habere göre de Aralık 2017'deZoobiaShahnazIŞİD'e göndermek için topladığı 62.000 dolarlık Bitcoin elde etmesinin ardından New York'da tutuklanmış, suçlu bulunduğunda banka dolandırıcılığından 30 yıl, her kara para aklama suçundan ise 20'şer yıl hapis cezasına çarptırılmıştır.

IŞİD'in terör eylemlerini finanse etmek için Bitcoin'i kullanması ise örgütün kripto para birimleri ile neler yapabileceğinin göstergesi olmuştur. Bir adım ilerisi olarak IŞİD'in üstlendiği Nisan 2019'da Paskalya zamanında Sri Lanka'da kilise ayinleri sırasında düzenlenen eş zamanlı saldırılarda 250'den fazla insan hayatını kaybetmiş, 400'den fazlada insanın yaralandığı terör eyleminin finansmanını örgütün Bitcoin ile gerçekleştirdiğine dair çarpıcı bulgulara ulaşılmıştır.

ABD vatandaşı olan birçok kişinin IŞİD'e Bitcoin ile finansman sağlamasının akabinde "*Bureau of Counterterrorism and Countring Violent Extremism*" departmanı Bitcoin ile terörist gruplar arasındaki ilişkiyi incelemeye başlamış, ancak Dark Web üzerinden işlemlerin gerçekleşmesi ise somut adımların atılması yönünde engel olmuştur. Sempatizanlar ve militanlar tarafından finansman sağlanmasına yönelik Bitcoin kullanımının bir adım ötesinde IŞİD'in terör eylemlerini finanse etmek için Bitcoin'i kullanması ise örgütün kripto para birimleri ile neler yapabileceğinin göstergesi olmuştur. Bir adım ilerisi olarak IŞİD'in üstlendiği Nisan 2019'da Paskalya zamanında Sri Lanka'da kilise ayinleri sırasında düzenlenen eş zamanlı saldırılarda 250'den fazla insan hayatını kaybetmiş, 400'den fazlada insanın yaralandığı terör eyleminin finansmanını örgütün Bitcoin ile gerçekleştirdiğine dair çarpıcı bulgulara ulaşılmıştır. CNN'de yayınlanan "*Breaking: ISIS Used Bitcoin to Fund Horrific Sri Lanka Easter Bombings, Research Claims*" isimli haberde İsrailli

bir blockchain firması olan Whitestream'ın yayınladığı bilgilere göre IŞİD'in Sri Lanka saldırı öncesi Bitcoin cüzdanının bulunduğu CoinPayments şirketindeki hesabındaki hareketliliği ifşa etmiştir.

Whitestream şirketi tarafından uzun zamandır IŞİD'e dair Bitcoin cüzdanlarının takip edilmesi, Sri Lanka saldırısında IŞİD'in ilgili şirketteki hesabından saldırıyı finanse ettiğine dair bulgulara ulaştıklarını belirtmişlerdir. Sonuç olarak IŞİD'in ulusların finansal kıskacından Bitcoin gibi kripto paralar ile kurtulduğu, eylemlerinin gerçekleştirilmesinde keşif, malzeme tedariği gibi hareketlerinde ise militanlarına kripto paralar üzerinden fon sağladığı anlaşılmıştır.

Saldırı öncesi hesapta bulunan 500.000 dolar 4.5 milyon dolar değerine ulaşmış, saldırı sonrası ise tekrardan 500.000 dolara düşmüştür. Söz konusu şirket büyük miktarda hesap hareketliliğini kabul etse bile IŞİD'in saldırıyı finanse ettiğine dair bilgilerinin olmadığını savunmuştur. Ancak Whitestream şirketi tarafından uzun zamandır IŞİD'e dair Bitcoin cüzdanlarının takip edilmesi, Sri Lanka saldırısında IŞİD'in ilgili şirketteki hesabından saldırıyı finanse ettiğine dair bulgulara ulaştıklarını belirtmişlerdir. Sonuç olarak IŞİD'in ulusların finansal kıskacından Bitcoin gibi kripto paralar ile kurtulduğu, eylemlerinin gerçekleştirilmesinde keşif, malzeme tedariği gibi hareketlerinde ise militanlarına kripto paralar üzerinden fon sağladığı anlaşılmıştır. Böylelikle de finansal araçların kullanımı kripto paralar ile Dark Web'de anonimlik üzerine gerçekleştiren IŞİD siber terörizmde yeni bir boyutun kapısını aralamıştır.

Siber Terörizm ve Yeni Güvenlik Sorunları

2019 yılında IŞİD'in Sri Lanka'da gerçekleştirmiş olduğu saldırıyı Bitcoin ile finanse etmesi, IŞİD

militanları ve sempatizanlarının Bitcoin ile örgüte para transfer etmesi siber terörizmin geldiği boyutu gözler önüne sermektedir. Fiziksel dünyada örgüt ağır darbeler almış olsa da siber alanda giderek aktifleşmiş ve bir terör eylemini siber alanda organize edebilecek seviyeye ulaşmıştır. Klasik terörizmden sonra en önemli güvenlik sorunu olarak karşımıza çıkan siber alandaki terörizm faaliyetlerininanonimlik esaslı olarak başta IŞİD olmak üzere devlet dışı silahlı aktörler tarafından gerçekleştirilmesi ise felaket senaryolarının ortaya çıkmasına sebep olmaktadır.

“Kripto para birimleri ile finansal ürünlere erişimin kolaylaşması finansal güçlenmeye yardımcı olmuş, yolsuzluk ve dolandırıcılık risklerini de minimize ederek hükümetlere ve kamu kuruluşlarına katkı sağladığı savı ortada olsa da, devlet dışı silahlı aktörler tarafından siber terörizm eylemleri için kullanımı siber terörizm ile mücadeleyi güçleştirmiştir.”

Siber alanda gerçekleştirilen saldırıların fiziksel dünyanın aksine tamamen anonim kalması mümkündür. Özellikle devlet dışı silahlı aktörlerin faaliyetlerini yürütmeleri için ihtiyaç duydukları finansmanı kripto paralar ile sağlamaları, anonimlik ile dijital paraların takibinin güçlüğü siber terörizm ile mücadeleyi güçlendiren unsurların başında yer almaktadır. Her ne kadar kripto para birimleri ile finansal ürünlere erişimin kolaylaşması finansal güçlenmeye yardımcı olmuş, yolsuzluk ve dolandırıcılık risklerini de minimize ederek hükümetlere ve kamu kuruluşlarına katkı sağladığı savı ortada olsa da, devlet dışı silahlı aktörler tarafından siber terörizm eylemleri için kullanımı siber terörizm ile mücadeleyi güçleştirmiştir. Dolayısıyla da kripto paralar ile ulusların uluslararası sistem içerisinde ortak bir hareket stratejisi belirlemeleri, siber alan ile ilgili tıpkı nükleer silahlar, biyolojik silahlarda olduğu gibi ortak bir anlaşma metinleri ortaya koymaları gerekmektedir. ■