İç Güvenlik Fakültesi Dergisi

ISSN: 3108-7248
Yıl: 2026, **Cilt:** 1, **Sayı:** 1, **Haziran** 2026 s. 117-139 **Makale Türü:** Araştırma
Makalenin Geliş Tarihi: 01.04.2026 **Makalenin Kabul Tarihi:** 25.06.2026

Balkanlar'da Siber Suçlarla Mücadele: iPROCEED ve CyberSee Projeleri

Burak Yağcı[1]

Öz: Balkanlar; coğrafi olarak Avrupa ve Asya kıtalarını birleştiren, tarihi itibariyle büyük devletler arasında sürekli paylaşım mücadelesine konu olan siyasi nüfuz alanı olarak şekillenmiştir. Söz konusu bölge, konumu gereğince Balkan Yarımadası'nda sosyolojik bakımdan farklı kültürleri tek bir potada eriten kozmopolit bir yapı kazanmıştır. Balkanlar'ın yer şekilleri itibariyle dağlık yapıda olması, burada yaşayan etnik ve dini grupların birbirinden bağımsız ve izole kalmasını sağlamıştır. Söz konusu parçalı yapı yerel kimliklerin korunmasının yanı sıra merkeziyetçi tek bir otorite altında toplanmayı da zorlaştırmıştır. Bu sebeple bugünkü siyasi coğrafyada Güneydoğu Avrupa'da konumlanan Balkanlar, siyasi çekişmeler bağlamında büyük bir önem arz etmiştir. Balkanlar merkeziyetsiz yönetim yapısı, coğrafi olarak çekişme alanı içinde olması ve teknolojik altyapı eksiklikleri nedeniyle zamanla organize suç örgütleri için ana hedef haline gelmiştir. Öyle ki stratejik konumu itibariyle bu bölge Avrupa'ya açılan bir kapı ve teknolojik silahların kullanıldığı deneme tahtası olarak görülmüştür. Organize suç ve dolandırıcılık faaliyetleri zamanla internet ortamına taşınmış ve bu kapsamda gerçekleştirilen siber saldırılar Balkanlar'da kritik altyapılar için yıkıcı etkiler doğurmuştur. Söz konusu yıkıcı etkiler bölgede kolektif bir güvenlik anlayışının gelişmesini zorunlu kılmıştır. Bu çalışmada, Balkanlar'da yeni bir güvenlik yaklaşımıyla internette işlenen suç gelirleri hedef alınarak dijital delillere ilişkin soruşturma, adli yardımlaşma ve teknik iş birliği hususları ele alınmıştır. Bölgede karşılaşılan siber suçlar incelenerek bu suçlarla mücadelede Avrupa Konseyi kapsamında yürütülen Iproceed ve CyberSee projeleri mercek altına alınmıştır. Söz konusu çalışmanın temel araştırma sorusu Balkanlar'da zamanla gelişen siber suçların bu bölgeye etkilerine karşı hayata geçirilen projelerin, Balkan ülkelerinin siber suçlarla mücadeledeki kurumsal ve hukuki kapasitelerine ne ölçüde katkı sağladığıdır. Makalede ele alınan hipotezin detaylandırılması amacıyla doküman incelemesi metodu kullanılarak ikincil veri analizi yöntemiyle siber suç istatistikleri analiz edilmiştir. Bununla birlikte literatür taraması yapılarak Avrupa Birliği, Avrupa Konseyi ve diğer kuruluşlar tarafından raporlanan siber suçlar ele alınmıştır.

Anahtar Kelimeler: *Balkanlar, Organize Suç, Siber Suç, İproceed, CyberSee*

[1] Burak Yağcı, Bilgi Teknolojileri ve İletişim Kurumu, Bilişim Hukuku Uzmanı, Doktora Öğrencisi, 0009-0003-9787-8791

Journal of Faculty of Homeland Security

ISSN: 3108-7248
Year: 2026, **Volume:** 1, **Issue:** 1, **June** 2026 p. 117-139 **Article Type:** Research
Received: 01.04.2026 **Accepted:** 25.06.2026

Combating Cybercrime in the Balkans: iPROCEED and CyberSee Projects

Abstract

The Balkans, geographically connecting the continents of Europe and Asia, have historically been a sphere of political influence, constantly contested by major powers. Due to its location, the region has developed a cosmopolitan structure on the Balkan Peninsula, blending diverse cultures into a single melting pot. The mountainous topography of the Balkans has ensured that ethnic and religious groups living there remain independent and isolated from one another. This fragmented structure has made it difficult to preserve local identities as well as to unite them under a single central authority. Therefore, in today's political geography, the Balkans, located in Southeast Europe, have held great importance in the context of political conflicts. Due to its decentralized governance, geographical location within a conflict zone, and lack of technological infrastructure, the Balkans have become a primary target for organized crime groups. Indeed, due to its strategic location, this region has been seen as a gateway to Europe and a testing ground for technological weapons. Organized crime and fraudulent activities have gradually moved to the internet, and cyberattacks carried out within this context have had devastating effects on critical infrastructure in the Balkans. These devastating effects have necessitated the development of a collective security approach in the region. This study examines a new security approach in the Balkans, targeting the proceeds of crimes committed online, and addresses issues of investigation, judicial assistance, and technical cooperation related to digital evidence. By examining cybercrimes encountered in the region, the Iproceed and CyberSee projects, implemented under the auspices of the Council of Europe, are analyzed in detail to combat these crimes. The main research question of this study is to what extent the projects implemented in response to the impact of cybercrime, which has developed over time in the Balkans, contribute to the institutional and legal capacities of Balkan countries in combating cybercrime. To elaborate on the hypothesis discussed in the article, cybercrime statistics were analyzed using secondary data analysis with a document review method. Furthermore, a literature review was conducted, examining cybercrimes reported by the European Union, the Council of Europe, and other organizations.

Keywords: *Balkans, Organised Crime, Cybercrime, Iproceed, CyberSee*

Giriş

Balkanlar, jeostratejik konumu ve önemli ulaşım güzergâhları üzerinde bulunması nedeniyle organize suç faaliyetlerinin yoğunlaştığı ve uluslararası suç ağlarının etkinlik gösterdiği başlıca bölgelerden biri olarak kabul edilmektedir. Öyle ki bu bölge uluslararası literatürde büyük devletler için Avrupa'ya açılan bir kapı ve tampon bölge hüviyetinde görülmektedir. Balkan coğrafyasında siyasi kurumsallaşma süreçlerinin kesintili bir seyir izlemesi ve yönetimsel kapasiteye ilişkin yapısal sorunlar, tarih boyunca çeşitli güvenlik sorunlarının ortaya çıkmasında etkili olmuştur. Bununla beraber Balkanların jeopolitik ve siyasi kırılganlıkları bölgede organize suç vakalarının artmasına da neden olmuştur. Dijitalleşme ile birlikte siber uzay bağlamında gerçekleştirilen siber saldırılarla bahse konu suçlar anonimleşmiştir. Bununla birlikte anonim ortam siber saldırganlar için güçlü bir motivasyon kaynağı haline gelmiştir. Geleneksel organize suç şebekelerinin yasa dışı eylemlerine siber saldırıları entegre etmesiyle bölgenin güvenlik yaklaşımında büyük bir dönüşüm yaşanmıştır. Özellikle de kaçakçılık, yasa dışı ticaret ve kara para aklama gibi geleneksel suçlar siber saldırılara entegre edilerek soruşturulması ve kovuşturulması zor bir süreç ortaya çıkarılmıştır. Bu çerçevede Balkanlar'da güvenlik algısı değişmiş ve hibrit tehditlerle beraber ele alınması gereken modern bir güç rekabeti oluşmuştur. Dolayısıyla Balkanlar'da ve Avrupa'da bölgesel siber kapasite inşası ve güvenlik yönetişimi ön plana çıkarılmıştır. Çalışmanın başlığında da yer verilen söz konusu projeler bölgesel siber güvenlik mimarisine entegre edilerek stratejik bir siber dayanışma ağı oluşturulmuştur. Öyle ki bu projeler neticesinde Balkanlar'da siber güvenlik alanında adli yardımlaşma ve teknik iş birliğine verilen önem artmıştır. Tüm bunlar ışığında geçmişten günümüze yaşanan dijital dönüşüm ile bölgedeki organize suç faaliyetlerinin siber suçlarla genişlemesi hususunun anlaşılması için bölgenin tarihi kökenleri ve siyasi olaylar büyük bir önem arz etmektedir. Bu sebeple söz konusu çalışmada ilk olarak Balkanların tarihsel ve siyasi süreci kısaca ele alınacaktır.

Balkanların Tarihi Kökenleri ve Siyasi Yapı

Tarihsel kronolojide 14. yüzyıldan 20. yüzyıl başlarına kadar Osmanlı Devleti topraklarının bulunduğu Balkanlar'da uygulanan iskân politikaları, tımar rejimi ve millet sistemi ile yalnızca belirli bir süreliğine güvenlikli toplum, merkeziyetçi idari yapı ve toprak işleme devamlılığı sağlanabilmiştir. Bununla birlikte sadık ordu ve bürokrasi içeren hoşgörülü bir idari yönetim anlayışı ortaya konmuştur. Ancak zamanla bu sistemlerdeki yozlaşma ile birlikte merkezi otorite bozulmuş ve ayanların ortaya çıkmasıyla yerel güvensizlik baş göstermiştir. Gayrimüslimler millet sistemi ile dinlerini özgürce yaşayabiliyorken etnik ve kimlik tabanlı bağımsızlık çabaları dolayısıyla bölgede karmaşık bir ortam meydana gelmiştir. Söz

konusu ortamda yayılmacı devletlerin kışkırtmalarıyla yerel milliyetçi akımlar ön plana çıkmıştır. Bu gelişmeler sonrası Osmanlı Devleti Balkanlar'da güç ve toprak kaybetmeye başlamıştır (Vucinich, s. 53-60).

19. yüzyılda Osmanlı'nın büyük devletler tarafından "hasta adam" olarak nitelendirildiği ve parçalandığı dönemde Balkanlar bahse konu milliyetçilik akımıyla toprak paylaşımlarına konu olmuştur. "Doğu Sorunu" olarak adlandırılan ve Osmanlı'nın topraklarını korumak adına denge politikası izlediği bu dönemde Rusya, İngiltere, Fransa ve Avusturya-Macaristan'ın çatışan siyasi çıkarlarının olduğu görülmüştür (Jelavich, 1983a, s. 301). Bu dönemde Balkanlar; savaşların, diplomatik pazarlıkların ve ulusal ayaklanmaların görüldüğü bir coğrafya görünümü kazanmıştır. Büyük devletler, Osmanlı Devleti içerisinde yaşayan gayrimüslim halkın haklarını korumak bahanesiyle Osmanlı Devleti'nin iç işlerine karışma hakları olduğunu iddia etmiştir. Özellikle bunlar arasında Pan-Slavist politikaları ile Slav-Ortodoks halkları kışkırtarak Osmanlı Devleti içerisindeki etnik grupların bağımsızlık kazanmalarına temel hazırlayan Rusya ön plana çıkmıştır. Rusya tarafından Akdeniz'e inme, boğazlara ve İstanbul'a hâkim olma, Balkanlar'da ve Avrupa'da siyasi nüfuz elde etme amaçlarıyla yola çıkılmıştır (Vucinich, s. 85). İngiltere ise Rusya'nın Akdeniz'e inmesini engellemek ve bölgedeki ticari yolları korumak hedefiyle hareket etmiştir. İstanbul ve Boğazlar, Balkanlar'a ve Akdeniz'e açılan kapı olarak bu iki devlet arasındaki paylaşım mücadelesinde önem arz etmiştir. Bu çerçevede Rusya, hem Akdeniz hem de Karadeniz'i içine alan stratejik geçiş koridorunu kontrolünde tutmaya çalışmıştır (Jelavich, 1983a, s. 215). Balkanlar'da görülen etnik ve kimliğe dayalı sorunlarla bağdaştırılabilecek ulusal bağımsızlık hareketleri yine bahse konu devletlerin rekabeti doğrultusunda şekillenmiştir. Özellikle Rusya'nın kışkırtıcı politikaları, bu devletin Balkanları parçalamayı amaçladığı şeklinde yorumlanmıştır. Bu kapsamda Osmanlının toprakları konu edilerek yapılan anlaşmalarda Rusya, Balkanlar'daki Ortodoks halkı koruma yetkisine erişmiş ve siyasi nüfuzunu Osmanlı Devleti'nin iç işlerine karışarak göstermiştir (Jelavich, 1983a, s. 385-386). Bununla birlikte İngiltere, Rusya karşısında Osmanlıyı bölgede bir tampon devlet olarak görmüş ve Hindistan'a giden deniz yollarını kontrol altına almak istemiştir. Fransa ise kendi çıkarları için Osmanlının toprak bütünlüğünü savunmuş ve ticari nüfuzunu koruma yolunu seçmiştir. Kendisini Katolik-Hristiyan halkların hamisi olarak gören Fransa, özellikle Osmanlının Kuzey Afrika ve Levant bölgelerini hedeflemiştir. Avusturya-Macaristan İmparatorluğu'na bakıldığında ise bu dönemde, içerisinde Sırpları barındırması dolayısıyla Rusya'nın Pan-Slavist politikalarından çekindiği görülmüştür. Bu sebeple Balkanlar'da iç istikrarı savunmuş ancak yine de güneydeki Bosna'ya doğru yayılmacı bir politika izlemekten de geri durmamıştır (Jelavich, 1983a, s. 212-213). Tüm bunlara rağmen Osmanlı Devleti bir denge siyaseti izleyerek toprak bütünlüğünü koruma yolunu seçmiştir. Osmanlılık kimliği güçlü tutulmaya çalışılsa da modernizasyon faaliyetleri neticesinde Balkanlar kademeli olarak kaybedilmeye başlanmıştır.

Birinci Dünya Savaşı sonrasında Osmanlı Devleti'nin yıkılması ve ulus devletlerin kurulmasıyla Balkanlar'da bağımsızlıklarını ilan eden yeni devletler yarı-kolonyal bir düzende büyük devletlerin himayesinde siyasi hayatlarına devam etmiştir (Marshall, 2015, s. 96). Parçalanarak bağımsızlıklarını kazanan Balkan devletleri için yeni bir kimlik tanımlamanın yanı sıra siyasi ve ekonomik bir sınav da ortaya çıkmıştır. İkinci Dünya Savaşı sonrası Doğu ve Batı blokları olarak belirginleşen yeni siyasi düzende, Yugoslavya'nın Sovyetler'den kopuşu ile Tito-Stalin ayrılığı gibi olaylar Amerika Birleşik Devletleri'ne (ABD) bu bölgede siyasi nüfuz elde etme fırsatı sunmuştur (Jelavich, 1983b, s. 350-351). Soğuk Savaş döneminde ise İkinci Dünya Savaşı neticesinde ABD tarafından Balkanlar siyasi nüfuz amacıyla hedeflenmiştir. Truman Doktrini kapsamında 1946-1949 yılları arasındaki Yunan İç Savaşı'na müdahalesi ABD'nin Balkanlar'daki etkisinin kurumsal başlangıcı sayılmıştır (Jelavich, 1983b, s. 332). 1960'lı yılların başında Yugoslavya'nın sosyalist devlet anlayışı ile Sovyetler'in kontrolü dışında hareket edip Bağlantısızlar Hareketi liderliğine oynaması da söz konusu durumu pekiştirmiştir (Jelavich, 1983b, s. 419).

Balkanlar'da yaşanan siyasi kaygılarla birlikte Arnavutluk, Bulgaristan, Romanya ve Yugoslavya çift taraflı politikalar yürütmeye başlamıştır. Bu minvalde bir taraftan Sovyet sistemi haricindeki devletlerle Kuzey Atlantik Antlaşması Örgütü (NATO) kapsamında kurulan siyasi ilişkiler, diğer taraftan Sovyetler ve diğer komünist devletler ile sosyalist Karşılıklı Ekonomik Yardımlaşma Konseyi (COMECON) ve Varşova Paktı gibi oluşumlara katılım ikilemi ortaya çıkmıştır (Jelavich, 1983b, s. 378). İlerleyen zamanlarda Soğuk Savaş ortamında ABD ve Rusya arasında derin bir siyasi ve askeri çekişme yaşanmış, Balkanlar'daki devletler bahse konu iki büyük güç tarafından siyasi nüfuz alanlarına çekilmeye çalışılmıştır. NATO ve Varşova Paktı arasında Balkan devletleri seçime yönlendirilmiş ve bu bölge adeta iki blok arasında sınır hattı oluşturmuştur. Özellikle 1952 yılında Yunanistan ve Türkiye'nin NATO'ya üye olması ve Bulgaristan, Arnavutluk ve Romanya'nın Sovyetler'in etkisi altında komünist sistemde kalması bu durumu kanıtlamaktadır. Diğer taraftan Yugoslavya'nın bağlantısız kalarak farklı bir yola evrilmesi, bu dönemde bahse konu siyasi ayrılıkları daha da derinleştirmiştir (Jelavich, 1983b, s. 357).

Balkanlar'da parçalı siyasi yapıyı oluşturan ve 90'lı yılların başından itibaren domino etkisiyle Yugoslavya'dan ayrılan küçük devletler için hem etnik sorunlar hem de kimlik problemleri baş göstermiştir. Ortodoks ve Katolik Hristiyanların beraber yaşadığı bu bölgede dinsel problemler de artır görülmüştür. Avrupa sınırları içerisinde Batı ve Doğu Hristiyanlığı olarak nitelenen dinsel ayrımla Balkanlar'ın ikiye bölündüğü gözlemlenmiştir. Kültürel fay hattı olarak nitelenen ve Roma İmparatorluğu'nun bölünmesinden beri süregelen bu ayrımcılık Yugoslavya'nın dağılmasıyla daha da belirginleşmiştir. Yine Avrupa Birliği (AB) üyeliği kapsamında Ortodoks kesimin ve Sovyet etkisindeki bölgelerin, AB üyeliğini ka-

bul eden mekanizma bağlamında geri plana atıldığı ortaya çıkmıştır (Huntington, 1996, s 160-161). Bu kapsamda tarihsel süreçte Kosova ve Sırbistan arasındaki siyasi gerilim, Bosna-Hersek özelinde yaşanan etnik bölünmeler ile Kuzey Makedonya'da gerçekleşen kimlik bunalımı Balkanlar'da karşılaşılan somut problemler olarak ön plana çıkmaktadır (Andreas, 2011). İlerleyen yıllarda Katolik Kilisesi›ne bağlı olan Hırvatistan'ın Avrupa Birliği'ne katılması, diğer Balkan ülkelerine göre kendisini daha "Avrupalı" olarak görmesine ve üstünlük söylemlerinde bulunmasına yol açmıştır. Slovenya da zamanla kendisini bahse konu Avrupalı kimliği ile karakterize etmeye başlamıştır. Diğer taraftan, Ortodoks Kilisesi'ne bağlı olan Sırbistan ve Karadağ bu ülkelere göre daha az medeni şeklinde sunularak Doğulu kimliklerinin ağır bastığı izlenimi yaratılmıştır. Buna karşılık Sırplar ise, Balkan Müslümanlarına kıyasla kendilerini daha "Batılı" olarak nitelendirmiştir (Asboth, 2025, s. 2-3) Söz konusu hususlar Balkanlar ve bölgenin güvenliğini siyasi, ekonomik ve sosyal açıdan büyük bir risk altına sokmuştur. Bu güvensizlik ortamı yayılmacı devletlerin bölge üzerinde rahatça uydu-devlet modelini hayata geçirmesini kolaylaştırmıştır. ABD ve Rusya gibi devletlerin bölgeye müdahale etmesine meşru zemin hazırlayan ana unsur ise 1970'lerden 90'lara kadar uzanarak Balkanları "Avrupa'nın Ötekisi" olarak nitelendiren yaklaşımın yaygınlaşması olmuştur. Söz konusu söylem, Balkan halklarının tam olarak Avrupalı görülmemesi ve "tamamlanmamış Avrupalı" şeklinde ifade edilmesine yol açmıştır (Vezenkov, 2006, s 70). Bu yaklaşımla Balkanlar, kurgulanan ve damgalanan bir bölge hüviyetinde büyük devletlerin paylaşım planlarına konu olmuştur. Ancak söz konusu nitelendirme Balkan milliyetçileri için olumlu yönüyle değerlendirilmiştir. Öyle ki bu söylem, Balkanlar'ın bir yandan Avrupa ile meşruiyet sağlayan bir ilişki sürdürmesini sağlarken diğer taraftan Balkan halklarının kendi kültürel kimliklerini koruyabilecekleri bir ortama imkân sağlamıştır (Vezenkov, 2006, s 70).

Bu bağlamda tarihi kronolojide tampon bölge konumunda bulunan Balkanlar'ın, Soğuk Savaş sonrası dönemde dönüşüme uğrayarak ABD ve Rusya ekseninde siyasi nüfuz alanı haline geldiği çıkarımı yapılabilecektir. Bölgede gerçekleşen jeopolitik kırılganlıklar dolayısıyla gerçekleşen siyasi parçalanma ile oluşan ekonomik ve sosyal değişimler belirli güvenlik risklerini de beraberinde getirmiştir. Özellikle merkezi otoritenin güç kaybetmesi ile gücü elinde bulunduran kesimlerin veya grupların kendi kurallarını uyguladığı parçalı bir yapı ortaya çıkmıştır. Diğer taraftan özellikle savaş zamanlarında büyük devletler tarafından teşvik edilen silah ticareti ve kaçakçılığının da gün yüzüne çıktığı görülmüştür. Güvensiz görülen bu ortamda bölgedeki konvansiyonel suçlar artış göstermiş ve yayılmacı devletler çeşitli örgütler aracılığıyla bölgeyi bir suç mahalline dönüştürmüştür. Dolayısıyla, devlet otoritesinden uzak gri alanlarda yasa dışı eylemlerde bulunan organize suç şebekeleri bu bölgeyi lojistik bir merkez sahasına çevirmiştir. Bilgi ve iletişim teknolojilerinin de gelişmesiyle bölgede görülen suç

çeşitliliği zamanla artarak güvenlik anlayışı farklı bir yaklaşımla ele alınmaya başlamıştır. Öyle ki klasik suçlar bu bölgede siber saldırılarla beraber daha yıkıcı bir etki doğurmaya başlamıştır. Özellikle kaçakçılık, yasa dışı ticaret ve kara para aklama gibi geleneksel suçlar siber saldırılara entegre edilerek soruşturulması ve kovuşturulması zor bir süreç ortaya çıkarılmıştır. Bu çerçevede Balkanlar'da güvenlik algısı değişmiş ve bölge hibrit tehditlerle beraber ele alınması gereken modern bir güç rekabeti alanına dönüşmüştür. Söz konusu güvenlik algısına ilişkin ayrıntılara aşağıdaki bölümde yer verilmektedir. Ancak bu ayrıntılardan önce Soğuk Savaş sonrası dönemde büyük devletler için bölgenin günümüzde kazandığı öneme değinilerek Balkanlar'ın son durumu ele alınacaktır.

Balkanlar'da Değişen Güvenlik Algısı ve Siber Suçlarla Mücadele

Balkanlar'da ekonomik ve siyasi nüfuz mücadelesinde, büyük devletlerin bölge üzerinde hakimiyet kurma motivasyonunun zamanla arttığı görülmüştür. Özellikle Soğuk Savaş sonrası ABD ve Rusya arasındaki siyasi hakimiyet mücadelesi burada kendisini göstermiş, Balkan devletleri daha önce de belirtildiği üzere AB ve NATO'ya üyelik ile Rusya'nın çıkarlarına hizmet eden uydu-devlet olma noktasında ikili bir yol ayrımına sürüklenmiştir. Söz konusu ayrım süreç içerisinde keskinleşmiş ve devletler arasında çarpıcı bir hibrit savaş ortamı meydana gelmiştir. Bahse konu hibrit savaş modelinde ise en önemli payı siber operasyonlar ve bilgi savaşlarının aldığı görülmüştür (Beraia, 2021). Söz konusu siber operasyon ve suçlara geçilmeden önce Balkanlar'da güvenlik algısının nasıl değiştiğine değinilmesi gerekmektedir. Bu kapsamda öncelikle bölgede ABD-Rusya ekseninde gelişen olaylara yer verilecektir.

Günümüzde Rusya-Sırbistan ilişkilerine karşılık ABD'nin Arnavutluk, Kosova ve Kuzey Makedonya ilişkileri modern dönemde de Balkanlar'daki siyasi nüfuz mücadelesinin sürdüğünü göstermektedir. Bu ülke halklarının özellikle AB ve NATO üyeliği konusundaki talepleri istatistiklere de yansımaktadır. Karadağ ve Bosna-Hersek'te ise düşük denemeyecek oranda bir kesimin ABD-Rusya arasında bir denge siyasetini benimsediği görülmektedir. Diğer taraftan Rusya için Balkanlar'da özellikle Sırbistan üzerinde hakimiyet kurma çabasının olduğu, bu kapsamda bölgede jeopolitik etkisini devam ettirmek istediği görülmektedir. Sırbistan'ın da tarihsel ve kimlik tabanlı problemler açısından bakıldığında derin bağları bulunan Rusya ile iyi ilişkiler kurmak istediği görülmektedir (Svetoka & Doncheva, 2021, s. 18-22). Rusya'nın siyasi ve ekonomik ortağı Çin'in ise AB'ye rakip olarak önemli finansal yatırımlar ile Balkanlar'da aktif olmaya çalıştığı istatistiklere yansımaktadır. Bu kapsamda Çin'in, Balkanlar'da ekonomik destek ve yatırım sağlayarak siyasi ve ekonomik bir nüfuz alanı sağlamaya çalıştığı yorumu yapılabilecektir (Svetoka & Doncheva, 2021, s. 18-22).

Diğer taraftan Avrupa-Atlantik entegrasyonu olarak nitelenen yapıda, Balkan ülkelerinin NATO ve AB'ye üyeliği gündeme getirilmektedir. Hırvatistan, Karadağ, Kuzey Makedonya ve Arnavutluk gibi devletlerin NATO üyesi olduğu, bununla Rusya'nın yayılmacı politikalarından askeri ve siyasi olarak uzak durmaya çalıştıkları yorumu yapılmaktadır (Marleku & Aliu, 2023, s. 190-196). Slovenya, Hırvatistan ve Bulgaristan'ın ise AB'ye üye yapılarak askeri güçlerinin yanı sıra hukuki alanda da dayanıklı hale gelmeleri ve reformsal gelişimlerinin sağlanmasının amaçlandığı vurgulanmaktadır. Bu kapsamda AB direktifleri ve normlarına uygun politikalarla bu devletlerin iç güvenlik ve istikrarının sağlanması hedeflenmektedir. Bu kapsamda organize suça ilişkin eylemler azaltılarak yolsuzluklar ve diğer suçlarla mücadele edildiği görülmektedir. Söz konusu Balkan devletlerinin NATO ve AB'ye birlikte üye olma yaklaşımı sergilemesi ise bölge istikrarına yönelik bir çabanın temsilini göstermektedir. Diğer taraftan, Rusya'nın hegemonyasında gelişen post-Sovyet yaklaşımının devre dışı bırakılması da üyelikle hedeflenen amaçlar arasında yer almaktadır (Rupnik, 2011, s. 27-30).

Rusya öncülüğünde gelişen Doğu Bloku'na bakıldığında ise Balkanlar üzerinde farklı siyasi ve ekonomik hedefler amaçlandığı görülmektedir. Bu kapsamda Rusya'nın Balkanlar üzerindeki etkisi genel olarak enerji arzı ve nakil hatları bağlamında ön plana çıkmaktadır. Öyle ki Balkanlar Rusya için Avrupa'ya uzanan bir enerji koridoru anlamı taşımaktadır. Buna karşılık ABD ise Rusya gazına bağımlılık içeren mevcut durumu tersine çevirmek için bu koridoru kontrolünde tutmaya çalışmaktadır. Doğal gaz boru hatlarının yanı sıra hem Ege hem de Adriyatik Denizi civarındaki deniz ticaret yolları ekonomik bakımdan bölgenin önemini artırmaktadır. Ekonomik eksenden bakıldığında Rusya ve Çin tarafından Balkan devletleri Batı yerine Doğu'ya entegre edilmeye çalışılmış ve özellikle enerji sektöründe önemli yatırım hamleleri gerçekleştirilmiştir. Bu kapsamda kredi ve serbest ticaret anlaşmaları yapılarak Balkanlarla mali entegrasyon sistemi kurulmaya çalışıldığı görülmektedir (Garčević, 2021 s. 4-6).

Tarihi yönden bakıldığında ise Yugoslavya Sosyalist Federal Cumhuriyeti'nin (YSFC) dağılması sonrası içerisindeki etnik sosyalist cumhuriyetlerin yeni devletler kurduğu görülmüştür. Buna rağmen Rusya tarafından ortak bir kökenin paylaşıldığı ve kültürel bağların devam ettirildiği söylemleri ile bahse konu cumhuriyetler üzerinde siyasi nüfuz kurulmaya çalışılmıştır. Bu kapsamda Balkanlar sadece jeopolitik ve ekonomik olarak değil aynı zamanda ortak kimlik ve tarih yaklaşımı içinde Ruslar tarafından Ortodoks-Slav dünyası anlayışı ile elde tutulmaya çalışılmıştır. Halen de bu tip söylemlerle Rusya, Sırbistan gibi ülkeler üzerinde etkisini devam ettirmektedir. Söz konusu yumuşak güç kullanımı özellikle "Küçük Ruslar" söylemi ile somutlaştırılmaktadır (Djokic, 2020, s. 233-235).

Balkanlar, daha önce de değinildiği üzere Doğu ve Batı Avrupa arasında konumlanması nedeniyle büyük bir önem arz etmektedir. Bu bölge coğrafi ve stratejik konumu itibariyle her iki kanadı birleştiren bir geçiş alanı ve tampon bölge

rolündedir. Bu sebeple bölge, Boğazlar ve Karadeniz etrafında kaçınılmaz bir mücadele alanı olarak nitelenmektedir (Hupchick, 2002, s. 2-3). Bölgenin stratejik önemi ve bahse konu olaylar güvenlik risklerini artırmış ve Balkanlar'ı Avrupa'nın güvensiz kanadı haline getirmiştir. Özellikle etnik sorunlar ile organize suç örgütlerinin artması bölgede yeni bir güvenlik problemini ortaya çıkarmıştır. Öyle ki Balkanlar, Avrupa ve Asya arasında uyuşturucu maddelerin nakli, insan ve silah kaçakçılığı gibi suça ilişkin organize eylemlerin coğrafi koridoru olarak tezahür etmiştir. Asya'dan Avrupa'ya uzanan Balkan rotası, Afgan eroin sevkiyatında stratejik bir kanal rolü üstlenmiştir. Söz konusu kanal vasıtasıyla AB'ye giden eroinin büyük bölümünün Balkan rotası ile sağlandığı ifade edilmektedir (Anastasijevic, 2005, s. 3-6).

Günümüzde söz konusu bölgede geçmişten gelen izlerle birlikte organize suç ve kaçakçılık olayları siber alana entegre edilmiştir. Dijitalleşme ile söz konusu organize suçlar siber saldırılarla desteklenmekte ve yıkıcı etkiler ortaya çıkmaktadır. Özellikle uyuşturucu, silah ve insan kaçakçılığı gibi suçlarda siber saldırılar araç olarak kullanılmaya başlanmıştır (Yağcı, 2023, s. 147). Bu kapsamda organize suç şebekeleri, bölgedeki zayıf güvenlik ağını ve devlet kırılganlıklarını da fırsat bilerek tehdit unsuru oluşturmaktadır. Batı Balkanlar'da organize suçlarda özellikle çevrim içi dolandırıcılık, kimlik hırsızlığı ve dijital kara para aklama gibi siber saldırılar bölgede siber suçluların kullandıkları en yaygın yöntemler arasında yer almaktadır (Buçaj et al., 2025, s. 5-6). Organize suçlar teknolojik gelişmelerle dijitalleşmiş ve suçlular anonim özellik kazanmak uğruna ileri düzey siber saldırı tekniklerini kullanmaya başlamıştır (Yağcı, 2023, s. 149). Özellikle Balkanlar'da Arnavut ve Sırp suç gruplarının dijital ve şifreli iletişim platformları aracılığıyla kara para aklama ve kaçakçılık gibi yasa dışı faaliyetler yürüttüğü görülmektedir. Söz konusu platformların yalnızca mesajlaşma için değil aynı zamanda lojistik, ödeme işlemi takibi ve kolluk kuvvetlerine yakalanmamak için araç olarak kullanıldığı da ifade edilmektedir (Zhilla, 2024, s. 19-20). Burada en sorunlu hususların başında ise bahse konu platformların ve dijital araçların, kabiliyeti olmamasına rağmen saldırıda bulunmak isteyen kötü niyetli kişilerin kullanımına hizmet olarak suç (crime-as-a-service) şeklinde sunulması gelmektedir. Öyle ki siber saldırganlar yetenekleri olmasa dahi bahse konu platformlar aracılığıyla yıkıcı siber saldırılar gerçekleştirebilmektedir (Zhilla, 2024, s. 19-20).

Tüm bunlar doğrultusunda bölgede siber suç sayısındaki artışın arkasında yatan ana sebebin siber saldırganların stratejik konumu itibariyle Balkanlar'ı Avrupa'ya uzanan arka kapı olarak görmesi söylenebilecektir. Avrupa'ya nazaran bu bölgedeki ülkeler, dijital altyapı güvenliğinde gelişememiş ve bu nedenle siber saldırılara karşı daha dirençsiz bir görüntü sergilemektedir. Diğer taraftan bölgede tarihsel süreçte görülen yolsuzluklar, suçluların cezalandırılmasındaki noksanlık ve devletlerin denetim eksikliği siber saldırganların motivasyonunu artırmaktadır. Kıtalar arası organize suç ve kaçakçılık rotasının tam ortasında bulunan bu

bölgede kara para aklama eylemleri Avrupa'ya göre daha kolay gerçekleştirilebilmektedir. Diğer taraftan Balkan ülkelerine yöneltilen siber saldırılar diğer büyük devletlere yapılabilecek olası saldırı sonuçlarına göre siyasi olarak daha hafif düzeyde karşılık bulmaktadır. Öyle ki büyük devletler, uğradıkları siber saldırıları isnat edilebildikleri takdirde bu atfı karşı devlete yönelik savaş ilanı olarak nitelendirebilmektedir. Ancak Balkan ülkeleri siyasi olarak söz konusu saldırılara sert düzeyde siyasi ve askeri cevaplar verememekte, bu saldırıları yanıtsız bırakmaktadır. Yine Balkanlar'a yöneltilen siber saldırılar, büyük devletlerin teknik bakımdan söz konusu siber saldırıları deneme fırsatı bulduğu alanlar olarak ön plana çıkmaktadır. Bu kapsamda konunun daha iyi anlaşılması için Balkanlar'da siber suç istatistiklerinin analiz edilmesinin önem arz ettiği değerlendirilmektedir.

Balkanlar ve Avrupa Bağlamında Siber Suçlar

Günümüzde organize suç şebekelerinin Balkanlar'da siber saldırıları aktif olarak kullanmaya başladığı görülmektedir. Buna ilişkin kurumsal raporların ortaya konulması durumun açıklanması için büyük bir önem arz etmektedir. Bu kapsamda AB çalışmaları çerçevesinde siber suçla mücadeleye ilişkin en önemli raporlardan birisi, organize siber suç tehditleri ile kolluk kuvvetlerine yönelik stratejileri içeren "İnternet Organize Suç Tehdit Değerlendirmesi"dir (IOCTA). Söz konusu değerlendirme, Avrupa Polis Teşkilatı Siber Suç Merkezi (Europol EC3) tarafından derlenerek yıllık şekilde yayımlanmaktadır. Değerlendirme raporunda siber uzaydaki teknik tehditlerle beraber hizmet olarak suç ve sektörde yasa dışı olarak elde edilen kazançlar konu edilmektedir. AB'yi etkileyen bahse konu tehditler analiz edilerek üye ülkelere istihbarat içeren faydalı bir kılavuz sunulmaktadır (Europol, 2024, s. 6). Bu kapsamda 2024 yılı IOCTA Raporu'nda siber saldırganların AB kapsamında en sık kullandığı siber saldırıların; fidye yazılımı saldırıları (ransomware), internet ortamında çocukların cinsel istismarı (child sexual exploitation) araçları ve çevrim içi dolandırıcılık (iSpoof) saldırıları şeklinde ortaya çıktığı görülmektedir. Kimlik avı saldırıları (credential harvesting) ve oltalama (phishing) saldırıları da siber saldırganlar için tercih edilen yöntemler arasındadır (Europol, 2024, s. 4). Verilere göre, AB genelinde çevrim içi siber saldırıların önceki yıllara göre sürekli bir artış gösterdiği tespit edilmiştir. Bu artışta yeni siber saldırı tekniklerinin ve teknolojilerin ortaya çıkışı etkili olmuş, siber saldırganların karanlık ağ (dark web) üzerinden piyasaya girişinde yükseliş olduğu görülmüştür. Özellikle de hizmet olarak suç pazarında yapay zekâ araçlarının devreye girmesi siber saldırı yeteneklerinin artmasına yol açmıştır. Yine bu çevrim içi siber saldırı oranının artmasında siber saldırganların uçtan uca şifreleme (E2EE) ve mesajlaşma uygulamalarını kullanmasının etkili olduğu ortaya çıkarılmıştır. Bununla birlikte kötü amaçlı büyük dil modellerinin (LLM) bahse konu saldırılarda kullanılması da yıkıcı bir etki alanı oluşturmaktadır (Europol, 2024, s. 8-11).

AB genelinde kolluk kuvvetleri (LEAs) tarafından yürütülen siber suç operasyonlarına bakıldığında "Hive Fidye Yazılımları"nın 2021 yılından 2024 yılına kadarki süreçte 80'den fazla ülkede 1.500'den fazla şirketi mağdur ettiği sonucuna ulaşılmıştır (Europol, 2024, s. 19). Diğer taraftan kolluk kuvvetlerinin başarılı operasyonlarıyla yalnızca tekil bir olayda dahi 120 milyon avro civarında fidye ödemesinin önüne geçildiği paylaşılmıştır (Europol, 2024, s. 19). Fidye yazılımı saldırılarında bitcoin türünden kripto para birimi yaygın şekilde kullanılmasına rağmen alternatif kripto paraların (altcoin) da yaygınlaştığı görülmüştür. Özellikle kripto varlıkları aklamak amacıyla yer altı bankacılığı (shadow banking) olarak nitelenen sistemin aktifleştiği ve kripto para kartlarının tekrar türeyerek takas hizmetlerinde suç amaçlı kullanıldığı tespit edilmiştir. Çevrim içi dolandırıcılık kapsamında raporda yer verilen ve somut bir olay olan "iSpoof.cc web sitesi" siber saldırısına ilişkin operasyonda siber saldırganların tutuklandığı ve ekonomik kaybın tahminen 115 milyon avronun üzerinde olduğu sonucuna ulaşılmıştır. Bu saldırılara ilişkin dark web pazarında ise 17 ülkenin katılımıyla gerçekleştirilen operasyon kapsamında ise 2 milyonun üzerinde dijital kimlik barındıran 1,5 milyondan fazla bot listesi ele geçirilmiştir (Europol, 2024, s. 29). Bunun yanı sıra yatırım dolandırıcılığı çerçevesinde bir platforma yönelik gerçekleştirilen operasyonda yaklaşık kaybın 89 milyon avro civarında olduğu ve saldırı kapsamında 33.000'den fazla mağduriyetin oluştuğu çıkarımı yapılmıştır (Europol, 2024, s. 30).

Buna ilişkin olarak "Avrupa Para Kuryesi Operasyonu (European Money Mule Action)" kapsamında 2023'te yürütülen operasyonda dünya genelinde 10.759 para kuryesi (money mule) ve 474 yönlendirici tespit edilerek 1.013 kişi tutuklanmış, bu kapsamda 32 milyon avro civarında ekonomik kaybın önüne geçilmiştir (Europol, 2024, s. 31). Rapor kapsamında ele alınan "EMPACT Ortak Eylem Günleri" çerçevesinde karanlık ağlardaki web siteleri, forumlar, pazar yerleri, mesajlaşma uygulamaları ve sosyal medya paylaşımları analiz edilerek ortak bir soruşturma faaliyeti yürütülmüştür. Bu soruşturmaya Arnavutluk, Bosna-Hersek, Kosova, Moldova, Karadağ, Kuzey Makedonya, Sırbistan ve Ukrayna katılım sağlamış, Üsküp'te yer alan JAD Koordinasyon Merkezi vasıtasıyla eş zamanlı operasyonlar koordine edilmiştir. Söz konusu operasyonlarda ateşli silah kaçakçılığına yönelik faaliyet yürüten 120 yasa dışı hesap tespit edilmiş, kolluk kuvvetleri tarafından 566 kişi tutuklanmıştır. Bu tutuklamaların 218'inin göçmen kaçakçılığı, 186'sının uyuşturucu kaçakçılığı, 69'unun ateşli silah kaçakçılığı ve 89'unun ise diğer bağımsız suçlara ilişkin olduğu sonucuna varılmıştır (Europol, 2024, s. 16). Diğer taraftan çocukların cinsel istismarı materyallerinin internet ortamında giderek arttığı ve belirli yapay zekâ araçlarıyla müstehcen içerikler üretildiği görülmüştür. Çevrim içi cinsel istismar ve şiddet içeren içeriklerin bahse konu yapay zekâ araçları ile kendi kendine üretildiği görülmüştür. Bununla birlikte söz konusu eylemlerin işleniş süreci araştırılmış ve siber saldırganların

özellikle çocukları dijital oyun ve popüler sosyal medya platformlarında tespit ederek güvenlerini kazandıkları tespit edilmiştir. Bu süreçte çocuklara ilişkin çeşitli manipülatif eylemlerle cinsel içerikli materyaller elde edilmiş ve tehdit amacıyla kullanıldığı görülmüştür (Europol, 2024, s. 25).

IOCTA 2025 raporunda ise bir önceki yıl raporuna ilişkin siber saldırıların farklı bir boyuta ulaştığı ve siber suç ekonomisi üzerinden kazanç sağlanarak verilere yetkisiz erişim sağlandığı tespit edilmiştir. Bununla birlikte söz konusu saldırılarda elde edilen verilerin ticaret konusu yapılması eğiliminin ortaya çıktığı aktarılmıştır. Bu kapsamda kişisel verilerin, siber suç ekonomisinin temelini oluşturan ana emtia konumunda olduğu ve özel-kamu ayrımı olmaksızın yetkisiz şekilde ele geçirildiği vurgulanmıştır (Europol, 2025, s. 9). Hedeflenen verilerin genellikle bulut ortamı gibi uzaktan hizmetlere ilişkin erişim bilgilerini, sosyal medya ve kişisel e-posta hesabı bilgilerini, finans ve bankacılığa ilişkin hizmetler ile devletler için kritik öneme sahip kamu yönetimi sistemlerindeki hassas bilgileri içerdiği ifade edilmiştir (Europol, 2025, s. 9). Siber saldırganların fidye yazılım saldırıları (ransomware), kimlik avı saldırıları (credential harvesting), kötü amaçlı yazılımlar (malware), oltalama saldırıları (phishing), web sitesi sahtekarlığı (website Spoofing), sanal kart kopyalama (skimming), sosyal mühendislik (social engineering) ve diğer siber saldırı yöntemlerini kullandığına değinilmiştir. Emtia olarak kabul edilen söz konusu verilerin dijital suç platformlarında satılarak bu alanın sektörleşme riski oluşturduğu görülmüştür. Daha önceki IOCTA raporunda da vurgulanan üretken yapay zekâ (genAI) türlerinin artması ve büyük dil modellerinin (LLM) sosyal mühendislik saldırılarında kullanılması da siber tehditlerin büyümesine yol açmıştır (Europol, 2025, s. 9-14).

Bu saldırılara ek olarak dağıtılmış hizmet reddi saldırıları (DDoS) gelişmiş kalıcı tehdit saldırıları (APT), köle bilgisayar ağları (Botnet), ortadaki adam saldırılarının (Man-in-the-middle) da özellikle işletmeler ve kamu kurumlarının sahip olduğu sistemleri kullanılamaz hale getirdiği görülmektedir. IOCTA 2024 ve IOCTA 2025 raporları beraber değerlendirildiğinde Balkanları içine alan bir coğrafyada Avrupa genelinde gerçekleşen siber saldırıların organize suçlarda araç olarak kullanıldığı görülmektedir. Bu kapsamda verinin bir emtia olarak nitelendirilerek siber suç ekonomisinin oluşturulduğu görülmektedir. Diğer taraftan yapay zekânın bu saldırılarda kullanıldığı ve gelecekte de siber suç sayısını artırma potansiyeline sahip olduğu sonucuna ulaşılmaktadır. Buna karşılık doğru ve verimli bir şekilde kullanıldığında yapay zekâ teknolojileri aracılığıyla, siber suçların engellenerek bahse konu istatistiklerin azaltılmasında kullanılabileceği de değerlendirilmektedir. Ancak günümüzde karşılaşılan senaryolarda fidye yazılımı saldırıları ile kötücül yazılım saldırılarının revaçta olduğu, çevrim içi dolandırıcılığın gün geçtikçe yaygınlaştığı ve yetkisiz erişim sağlanan sistemlerin ele geçirilerek çeşitli platformlarda ticari satışa konu edildiği görülmektedir.

Diğer taraftan Avrupa Birliği Siber Güvenlik Ajansı (ENISA) tarafından yıllık olarak yayımlanan "Tehdit Ortamı Raporu" (Threat Landscape Report) kapsamında Avrupa'da meydana gelen siber güvenlik olayları ve tehditlerine ilişkin bir değerlendirme sunulmaktadır (ENISA, 2025, s. 5). Rapor; siber tehditlerin yanı sıra yeni siber suç eğilimleri, siber saldırı yöntemleri, "Birlik Genelinde Yüksek Ortak Siber Güvenlik Düzeyine Yönelik Önlemler Hakkında Direktif" (NIS2 Directive) kapsamında belirlenen kritik altyapı sektörlerine yönelik siber saldırılar ve bu saldırılara yönelik stratejilerin belirlendiği bir kılavuz görevi de görmektedir (ENISA, 2025, s. 15) Avrupa genelinde gerçekleşen siber saldırı istatistiklerine bakıldığında siber suçların tüm suç kategorileri içinde gerçekleşen olayların %13,4'ünü oluşturduğu, siber suçlar arasında ise saldırıların %81,1'inin fidye yazılımı (ransomware) saldırılarından meydana geldiği, geriye kalan oranın %15,2'sinin fidye yazılımı kaynaklı veri ihlalleri (data breach) kaynaklı olduğu görülmektedir (ENISA, 2025, s. 28). Söz konusu fidye yazılımı siber saldırılarının hedeflediği ana sektör %14,9 oranla üretim (imalat) sektörü olarak tespit edilmiştir. Bu sektörü dijital altyapı ve hizmetler sektörü %10,3 oranıyla takip etmiştir (ENISA, 2025, s. 31). Fidye yazılımı siber saldırıları bahse konu sektörlerde barındırılan verilerin gizlilik, bütünlük ve erişilebilirliğini etkileyerek sektörde ekonomik ve operasyonel düzlemde yıkıcı etki oluşturmuştur. Bununla birlikte Avrupa genelindeki veri ihlali saldırılarında dijital altyapı ve hizmetler sektörünün %28,2 oranıyla ilk sırada etkilendiği, bu sektörü ise kritik hizmetlerin de yer aldığı kamu yönetimi sektörünün %16,8 oranıyla takip ettiği ifade edilmiştir (ENISA, 2025, s. 31). NIS2 Direktifinde de yer alıp saldırılardan etkilenen diğer kritik altyapı sektörlerine bakıldığında ise iş hizmetleri, finans, ulaşım, sağlık, gıda ve enerji sektörlerinin ön planda olduğu görülmektedir (ENISA, 2025, s. 30).

Bahse konu siber saldırılar neticesinde elde edilen verilerin siber suç pazarları, forumlar ve dark web üzerinden satılması hedeflenmektedir. Bu kapsamda istikrarlı bir tehdit unsuru olarak siber saldırıların hem siber suçlar hem de organize suçlarda kullanılmaya devam edildiği görülmektedir. Özellikle kimlik hırsızlığı saldırıları ile kullanıcıların oturum bilgileri ele geçirilmekte, yetkisiz erişim vasıtasıyla kötü amaçlı yazılımlar satış platformlarında hizmet olarak pazarlanmaktadır. Bu kapsamda hizmet olarak fidye yazılım saldırılarının (RaaS) satışı ön plana çıkmaktadır. Öyle ki bu satışlarla siber yeteneklere sahip olmayan saldırganlar dahi gerekli donanıma sahip olmakta ve yıkıcı siber saldırılar gerçekleştirebilmektedir (ENISA, 2025, s. 28). Diğer taraftan bahse konu siber saldırılar neticesinde ilk erişim aracıları (IAB) tarafından yapılan satışlara ilişkin ekonomik modelde bir dönüşüm yaşandığı görülmektedir. Bu dönüşümün önceki satışlara göre düşük maliyetli ve yüksek hacimli olmaya başladığı tespit edilmektedir. Buna ilişkin olarak raporda erişim fiyatlandırmasının 2.800 avro eşiğinin altında olduğu ifade edilmektedir (ENISA, 2025, s. 29). IAB tarafından gerçekleştirilen satış faaliyetlerinin Avrupa genelinde yaygınlık kazandığı ve 2024 yılında gizlilik ve anonim-

lik sağlayarak coğrafi sınırları aşmaya yardımcı olan sanal özel ağ (VPN) erişim satışlarının ciddi düzeyde artış gösterdiği aktarılmaktadır. Bunun yanında raporda, kişisel olarak tanımlanabilir bilgiler (PII) ve uzak masaüstü protokolü erişim satışlarının önceki dönemlere göre aynı düzeyde kaldığı tespiti yapılmaktadır (ENISA, 2025, s. 30).

Avrupa Konseyi tarafından kara para aklamayı önlemek ve terörizmin finansmanıyla mücadele etmek amacıyla kurulan "Kara Paranın Aklanmasının Önlenmesine Yönelik Tedbirlerin Değerlendirilmesi ve Terörizmin Finansmanı ile Mücadele Uzmanlar Komitesi (MONEYVAL)" tarafından yıllık olarak yayımlanan değerlendirme raporlarında ise; bahse konu eylemlerin çoğunlukla organize suç örgütleri tarafından gerçekleştirildiği ve son yıllarda siber saldırıların bu eylemlere entegre edildiği görülmektedir. Raporlarda Avrupa'yı da etkileyen söz konusu siber saldırıların Balkanlar özelinde yıkıcı sonuçlar doğurduğu aktarılmaktadır. Buna ilişkin yayımlanan verilerde Arnavutluk olayı örnek verilerek gerçekleştirilen siber saldırılarda çevrim içi ortamda kredi kartı dolandırıcılığı vakalarının arttığı ifade edilmektedir (MONEYVAL, 2012, s. 23). Bununla birlikte Slovenya'da bilgisayar sistemlerine yetkisiz erişim sağlayarak kara para aklama olaylarının yaşandığı ve daha önce buna ilişkin tutuklamaların gerçekleştirildiği vurgusu yapılmaktadır. Olaya ilişkin soruşturmalarda muhtemel suç gelirinin 128.500 avro civarında bir hacme sahip olduğu ve söz konusu miktara sahip hesapların bir kısmının bloke edildiği ifade edilmiştir. Bu siber saldırılarda kötü amaçlı yazılım kullanıldığı ve fiilî olarak ekonomik kaybın 30.000 avro üzerine çıktığı tahmini yapılmıştır (MONEYVAL, 2012, s. 24). Bunlara ek olarak Romanya menşeili gerçekleşen daha önceki siber saldırılarda klavye kaydedici (keylogger) kötü amaçlı yazılımı ve sahte kimlikle kredi kartı hırsızlığı yapıldığı vurgulanmıştır. Bu saldırılarda ana hedefin kara paranın aklanması olduğu ve siber saldırganların 100 kredi kartına ait erişim bilgisi için 1000 ABD Doları istediği bilgisi verilmiştir (MONEYVAL, 2012, s. 41). Para aklamada kullanılan yöntemler için genellikle para kuryesi (money mule) araçları, oltalama saldırıları (phishing) ve klavye kaydedici (keylogger) kötücül yazılımların kullanıldığı aktarılmıştır (MONEYVAL, 2012, s. 48). Yasa dışı kara para aklama işlemlerinde ise para havalesi sağlayıcılarının operasyonlarda etkin şekilde yer aldığı bilgisi verilmiştir. Siber saldırılar neticesinde elde edilen suç gelirlerinin aklanmasında kripto ve dijital paraların düşük maliyet içermesi, transferde kolaylık sağlaması ve anonim özellikleri dolayısıyla sıklıkla kullanıldığı belirtilmiştir (MONEYVAL, 2012, s. 40-41).

Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte Sözleşmesi) Komitesi (T-CY) tarafından hazırlanan raporda ise Balkan ülkelerinin siber suçlarla mücadelede uluslararası iş birliği ve adli yardımlaşma kapsamında yaşadıkları vakalar ortaya koyulmaktadır. Bu kapsamda üyeler arasında teknik ve adli yardımlaşmaya imkân veren Budapeşte Sözleşmesi'ne Balkanlar'da Bulgaristan, Bosna Hersek, Hırvatistan, Yunanistan, Karadağ, Kuzey Makedonya, Sırbistan, Slovenya ve Tür-

kiye'nin üye olduğu görülmektedir (Council of Europe Cybercrime Convention Committee [T-CY], 2020, s. 45). Raporda, Bulgaristan resmi yetkilileri tarafından kötü amaçlı yazılım içeren siber saldırılarla gerçekleştirilen bir kara para aklama ve dolandırıcılık soruşturması paylaşılmıştır. Bahse konu olayı aydınlatmada faydası görülen yurt dışındaki bir şirketten dolandırıcılıkta kullanılan kripto para biriminin izlenmesi ve dondurulması kapsamında talep edilen yardım vakası incelenmiştir. Yaşanan siber olayda Budapeşte Sözleşmesi kapsamında uluslararası adli yardımla ilgili 35. madde devreye girmiş ve bu vaka sınır ötesi işlemlerde iş birliğinin önemini göstermiştir (T-CY, 2020, s. 15-16). Diğer bir olayda ise dijital dolandırıcılık faaliyeti kapsamında Bosna Hersek yetkili makamlarınca yürütülen soruşturma çerçevesinde e-posta hesap verilerinin korunması amacıyla yurt dışında yerleşik bir teknoloji şirketinden aynı madde kapsamında adli yardım isteminde bulunulduğuna yer verilmiştir. Bosna Hersek Savcılığı tarafından Budapeşte Sözleşmesi'nin 29. maddesi gereğince veri koruma taleplerinin iletildiği aktarılmıştır. Bu taleplerin dayanakları arasında şantaj, bilgisayar verilerine ve programlarına zarar verme, yetkisiz erişim, bilgisayar dolandırıcılığı, çocuk istismarı ve telif haklarının izinsiz kullanımının bulunduğu görülmüştür. Söz konusu olayda diğer ülkelerdeki internet servis sağlayıcılar tarafından talep edilen içerik ve trafik veri bilgisinin iletilmesi ile soruşturmanın hızlı bir şekilde devam etmesinin sağlandığı hususuna vurgu yapılmıştır (T-CY, 2020, s. 19). Bunun gibi bir diğer örneğe de Romanya'nın 7/24 irtibat noktası görevini yürüten ve Organize Suç ve Terör Suçlarını Araştırma Müdürlüğü (DIICOT) altında faaliyet gösteren Siber Suçlarla Mücadele Servisi özelinde rastlanılmıştır. Öyle ki bu Servis tarafından açıklanan 2019 yılı istatistiklerinde bilgisayar verilerinin saklanması amacıyla 144 talep alındığı ve 39 karşı talepte bulunulduğu ifade edilmiştir. Bununla beraber siber suç davalarında 407 adet karşılıklı hukuki yardım talebinde bulunulduğu bilgisi aktarılmıştır. Sağlanan bilgiler ve adli yardımlaşma ile gerekli delillerin toplanmasının siber saldırganların yakalanmasını kolaylaştırdığı ifade edilmiştir (T-CY, 2020, s. 16). 2020 yılında gerçekleşen ve Sırbistan, Bulgaristan, Avusturya, Almanya ve Eurojust'ın da destek verdiği bir operasyon kapsamında yatırım dolandırıcılığıyla siber suç işleyen iki organize suç grubuna yönelik tutuklama işlemi gerçekleştirildiği ve şirketin banka hesabında bulunan 2,5 milyon avro meblağın dondurulduğu aktarılmıştır. Söz konusu operasyon kapsamında Budapeşte Sözleşmesi'nin 26. maddesi çerçevesinde diğer paydaş ülkelerle bilgi paylaşımı yapılmıştır (T-CY, 2020, s. 17). Raporda, Türkiye'nin diğer üyelerden aldığı veri koruma taleplerinin sayısı raporun yazıldığı 2020 yılına kadarki dört yıllık süreçte 43 olarak kayda geçilmiştir. Diğer taraftan bu taleplerin 21'inin koruma kapsamında işleme alındığı, geri kalan taleplerin büyük bir kısmının ise verilerin mevcut olmaması veya teknik problemler sebebiyle geri çevrildiği ifade edilmiştir (T-CY, 2020, s. 21).

Çalışmada yer verilen bahse konu sözleşme ve raporlar çerçevesinde Balkanlar'ın, Avrupa ile olan doğal bağlantısı dolayısıyla organize suç şebekeleri ve siber suçların merkezi haline geldiği görülmektedir. Daha önce bahsedildiği üzere Balkanlar'ın 1990'lı yıllar sonrasında siyasi olarak parçalanması ve burada ortaya çıkan yeni devletlerin kimlik bunalımı içerisindeyken uydu-devlet modeline yöneltilmesi söz konusu tehditlerin yayılmacı devlet çıkarları doğrultusunda şekillendiğini göstermektedir. Özellikle bu bölümde yer verilen raporlardaki siber suç istatistikleri, bu bölgenin klasik suçlara entegre olan siber saldırıların açık hedefi konumunda olduğu görüşünü perçinlemektedir. Bölgede faaliyet gösteren organize suç örgütlerinin kaçakçılık ve uyuşturucu ticareti gibi yasa dışı eylemlerden elde ettikleri gelirlerin siber araçlar vasıtasıyla meşrulaştırıldığı görülmektedir. Öyle ki söz konusu yöntemlerle failler anonimlik sağlamakta, yasa dışı gelirler finansal perde görevi üstlenen kripto varlıklar ve dijital ödeme sistemleri aracılığıyla aklanmaktadır. Bu çerçeveden bakıldığında Balkanlar'da ulusal güvenlik yapılarının söz konusu saldırılara karşı yetersiz hale geldiği görülmektedir. Bahse konu zayıf ulusal güvenlik yapıları hem hukuki yetersizlikleri hem de dijital varlıklara ilişkin merkezi denetim noksanlığını göstermektedir. Bu sebeple Balkan ülkeleri sınır aşan tehditlerle mücadelede siber uzay bağlamında kolektif bir savunma yaklaşımını gerekli bulmuştur. Bahse konu müşterek savunma anlayışı kapsamında Avrupa Birliği ve Avrupa Konseyi tarafından birtakım projeler hayata geçirilmiştir.

Balkanlar'da Siber Suçlara Karşı Yürütülen Avrupa Projeleri

Organize suçlarda kullanılan siber saldırı araçlarına karşı müşterek siber savunma projelerinin hayata geçirilmesi siber suç istatistikleri göz önünde bulundurulduğunda zamanla daha fazla önem arz etmeye başlamıştır. Özellikle son on yılda bölge genelinde gerçekleşen siber saldırılarla organize suç ağı üyelerinin soruşturulması ve kovuşturulmasının zorlaştığı görülmüştür. Söz konusu organize eylemlere yönelik müşterek projelerin geliştirilmesi bölge güvenliği açısından gerekli olmuştur. Diğer taraftan, Balkanlar ve Avrupa'nın organik birlikteliği göz önünde bulundurulduğunda Avrupa ülkeleri tarafından kendi bölgeleri hedeflenerek gerçekleştirilen siber saldırılara karşı bu projeler finansal ve operasyonel olarak desteklenmeye başlanmıştır. Bu kapsamda Avrupa Birliği ve Avrupa Konseyi tarafından siber suçla mücadele, suç gelirlerinin aklanmasının önüne geçilmesi ve dijital delil güvenliği çerçevesinde stratejik müdahale aracı olarak yürütülen projeler hayata geçirilmiştir.

2016-2019 yılları arasında Avrupa Konseyi ile Avrupa Birliği'nin "IPA II Çok Ülkeli Eylem Programı" kapsamında ortak olarak yürüttüğü proje olan "Güneydoğu Avrupa ve Türkiye'de İnternet Üzerinden İşlenen Suç Gelirlerinin Hedef Alınması Projesi-iPROCEEDS" bu alanda ilk adım olarak ön plana çıkmıştır.

Proje, Avrupa Konseyi Siber Suç Program Ofisi (C-PROC) tarafından yürütülmüş ve bölge genelinde operasyonel seviyede uygulanmıştır. Bu projenin geçerlilik süresi 42 ay olmakla birlikte projeye finansal olarak 5,56 milyon avro bütçe tahsis edilmiştir. iPROCEEDS projesinin uygulama alanında katılımcı ülkeler arasında Arnavutluk, Bosna-Hersek, Karadağ, Sırbistan, Kuzey Makedonya, Türkiye ve Kosova bulunmaktadır. Söz konusu projenin amacı "IPA bölgesindeki yetkililerin siber suç gelirlerini aramak, ele geçirmek ve müsadere etmek ve internette kara para aklamayı önleme kapasitesini güçlendirmek" olarak ifade edilmiştir. Bu kapsamda siber suçlarla ilgili "Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte Sözleşmesi-CETS 185)" ve "Suç Gelirlerinin Aklanması, Araştırılması, El Konulması ve Müsaderesi ile Terörizmin Finansmanına İlişkin Sözleşme (CETS 198)" ele alınarak proje üyesi ülkelerde bilgi ve iletişim teknolojilerinin kullanımı ile elde edilen suç gelirlerini aklamanın önüne geçilmesi hedeflenmiştir. Organize suç örgütlerinin siber faaliyetler ve çevrim içi dolandırıcılık yöntemleriyle hem Balkanlar'da hem de Türkiye'de yasa dışı gelir elde ettiği ve bu projenin bölge açısından kritik bir öneme sahip olduğu belirtilmiştir (Council of Europe, Cybercrime Programme Office [C-PROC], 2019 s. 1). Projenin çıktıları arasında özellikle çevrim içi dolandırıcılık faaliyetleri ve siber suçlar kapsamında kamuya yönelik raporlama sistemlerinin hayata geçirilmesi gerekliliği ortaya konmuştur. Bununla birlikte proje ülkelerinde verilerin korunması çerçevesinde siber suç gelirlerine yönelik arama, el koyma ve müsadere tedbirleri hayata geçirilmiştir. Diğer taraftan internette kara para aklama faaliyetlerine ilişkin mevzuat altyapısı güçlendirilmiştir. Yine proje üyesi ülkelerdeki siber suç birimleri, mali soruşturma büroları, istihbarat birimleri ile koruma tedbirleri ve müsadereye ilişkin ulusal iş birliğinin sağlandığı aktarılmıştır. Bu kapsamda kamu-özel iş birliği çerçevesinde istihbarat değişim mekanizmalarının Balkanlar genelinde güçlendirildiği vurgulanmıştır. Diğer bir proje çıktısına bakıldığında ise finans sektöründe faaliyet gösteren kuruluşların çevrim içi dolandırıcılıktan korunması ve kara para akışlarının önlenmesine yönelik kılavuzlar geliştirildiği ifade edilmiştir. Yargı alanında elektronik deliller ve soruşturmalar hakkında eğitimler verildiği, adli iş birliğinin uluslararası boyutta geliştirildiği sonucu paylaşılmıştır (C-PROC, 2019, s. 2-3).

2020-2023 yılları arasında önceki projenin devamı olarak yine finansörlüğünü Avrupa Konseyi ile Avrupa Birliği'nin yaptığı ve ilk projede katılımcı ülkelerin (Arnavutluk, Bosna-Hersek, Karadağ, Sırbistan, Kuzey Makedonya, Türkiye ve Kosova) buraya da iştirak ettiği, 42 ay süren ve 4.945.000 avro bütçe tahsis edilen "Avrupa Birliği ve Avrupa Konseyi›nin Güneydoğu Avrupa ve Türkiye›de İnternet Üzerinden Elde Edilen Suç Gelirlerinin Hedeflenmesi ve Elektronik Delillerin Güvence Altına Alınması Projesi- iPROCEEDS-2" hayata geçirilmiştir. Bahse konu ikinci proje de temelinde ilk iPROCEED projesiyle aynı hedefleri taşımaktadır. Balkan ülkelerinin karşılaştıkları siber suç tehditleri çerçevesinde "Güneydoğu Avrupa Organize Suç Tehdit Değerlendirmesi" (OCTA SEE) sonuçlarında

bu bölgede siber suç sayısının ciddi bir artış gösterdiği ve ticari bir pazarın oluştuğu aktarılmıştır. Bu değerlendirmede; bilgisayar dolandırıcılığı ve sahteciliği, veri müdahalesi ve kişisel verilerin kötüye kullanılması, dağıtılmış hizmet reddi (DDoS) saldırıları, mobil cihazlara yönelik siber saldırılar, kötü amaçlı yazılımlar (malware), ATM kötü amaçlı yazılımları, çevrim içi dolandırıcılık, fidye yazılımı (ransomware) saldırıları, kripto para veya cüzdan adresi ele geçirme, SIM kutusu (box) dolandırıcılığı, kimlik hırsızlıkları, yönetici (CEO) dolandırıcılıkları, diğer ödeme dolandırıcılıkları ve çocukların çevrim içi cinsel istismarına yönelik siber saldırıların had safhaya ulaştığı bildirilmiştir. Söz konusu siber saldırılarda özellikle bitcoin gibi kripto para birimlerinin kullanıldığı ve kara para aklandığı vurgulanmıştır. Proje kapsamında verilerin korunmasına yönelik elektronik delillerin güvenceye alınması çerçevesinde faaliyetler yürütülerek mevcut mevzuatın güçlendirildiği aktarılmıştır (Council of Europe, Cybercrime Programme Office [C-PROC], 2022, s.1). Bu süreçte yetkili makamlar vasıtasıyla koordineli bir şekilde siber suç politika ve stratejilerinin hayata geçirildiği, özellikle siber olay raporlama ve Bilgisayar Güvenliği Olay Müdahale Ekipleri (CSIRT's) ile Bilgisayar Acil Durum Müdahale Ekipleri'nin (CERT's) veri paylaşımı için devreye sokulduğu vurgulanmıştır. Siber saldırılara ilişkin olası tehditlerin önlenmesi amacıyla ulusal CERT'ler arasında simülasyon çalışmaları gerçekleştirildiği ve siber suça yönelik eğilimler ile ceza adaleti konusunda raporlanmış istatistiklerin sunulduğu bilgisi verilmiştir. Balkanlar'da en az iki proje ülkesinde siber suç ve çevrim içi dolandırıcılıkla ilgili dijital raporlama sistemi kurulması hedeflendiği aktarılmıştır. Bu ülkelerin Kuzey Makedonya ve Kosova olması konusu desteklenmiş ve ABD'de faaliyet gösteren IC3 İnternet Suç Şikayetleri Merkezi'nin örnek alınması gerekliliği ifade edilmiştir. Diğer taraftan Avrupa Siber Suç Eğitim ve Öğretim Grubu (ECTEG) çalışmaları kapsamında siber suç ve mali soruşturmalara ilişkin atölye faaliyetleri, eğitimler ile siber güvenlik tatbikatlarının gerçekleştirilmesi hedeflenmiştir. Özellikle de sanal para birimleri ve dark web gibi alanlarda siber suç soruşturmalarının yürütülmesine dair vaka simülasyon çalışmaları planlanmıştır. Bu doğrultuda özellikle elektronik delillere yönelik yargı ve kolluk birimleri ile çok uluslu hizmet sağlayıcılar (MSP'ler) arasında iş birliğinin güçlendirilmesi gerekliliği paylaşılmıştır. Yine bununla birlikte Balkanlar'da ve uluslararası çapta dava simülasyon çalışmaları, masa başı tatbikatları ve platformlar kurulması hususları vurgulanmıştır (C-PROC, 2022, s. 2-6).

2024 yılının ocak ayı itibariyle Avrupa Birliği (DG NEAR) ve Avrupa Konseyi'nin ortak çalışması olarak başlatılan "CyberSEE: Güneydoğu Avrupa ve Türkiye'de Siber Suç ve Elektronik Delillere İlişkin Geliştirilmiş Eylem Projesi" ise iPROCEED I ve II projelerinde olduğu gibi Arnavutluk, Bosna-Hersek, Karadağ, Kuzey Makedonya, Sırbistan, Türkiye ve Kosova ülkelerinin katılımıyla 42 ay sürecek olup 30 Haziran 2027'de son bulacaktır. Bahse konu projenin bütçesi 5.500.000 avro olarak belirlenmiştir. Projenin uygulayıcısı, diğerlerinde olduğu

gibi Avrupa Konseyi Siber Suç Program Ofisi (C-PROC) olarak belirlenmiştir. Bu kapsamda Balkanlar ve Türkiye'de karşılaşılan siber suçlara ilişkin elektronik deliller hakkında hukukun üstünlüğü, güvenliği ve bölgesel iş birliğini güçlendirmek amaçlanmaktadır. Projenin neticelenmesi sonrasında hedeflenen çıktılar arasında Budapeşte Sözleşmesi ve Sözleşme'nin İkinci Protokolü kapsamında siber suç ve elektronik delillere yönelik mevzuatın iyileştirilmesi, siber strateji politikasının oluşturulması, ceza adaleti makamları tarafından gerçekleştirilen soruşturma ve kovuşturma mekanizmalarının geliştirilmesi ve son olarak bahse konu makamların siber güvenlik çerçevesinde diğer paydaşlarla olan iş birliğinin güçlendirilmesi yer almaktadır. CyberSEE kapsamında diğer iki projeye ek olarak fidye yazılımı saldırıları neticesinde siber saldırganlarca ele geçirilen sanal para birimlerine ilişkin arama, el koyma ve müsadereye ilişkin soruşturmaların geliştirilmesi, çevrim içi çocuk cinsel istismarı kapsamında detaylı soruşturma yapılması, bilgisayar sistemlerinde yer alan delillerin güvenceye alınması ve ceza adaleti makamları ile siber paydaşlar arası iş birliğinin daha ileri bir noktaya getirilmesi hedeflenmektedir (Council of Europe, Cybercrime Programme Office, 2024).

iPROCEED ve iPROCEED II projelerinin, özellikle Batı Balkanlar ve ülkemizin dijitalleşme ile birlikte karşı karşıya kaldığı siber suçlarla mücadelede önem arz ettiği değerlendirilmektedir. Öyle ki bahse konu projelerde siber suçlar vasıtasıyla kolaylaşan organize suçlardan elde edilen yasa dışı suç gelirleri tespit edilerek gerekli yaptırımlar uygulanmaktadır. Bu yaptırımlar arasında söz konusu gelirlere bağlı hesapların dondurulması ve malların müsadere edilmesi de yer almaktadır. Bunların da ötesinde ulusal yargı makamları tarafından faillere yönelik hürriyeti bağlayıcı cezalara hükmedilebilmektedir. Diğer taraftan bu projelerle uluslararası seviyede finansal ve hukuki iş birliği sağlanarak adli makamlar ve istihbarat birimlerine yönelik siber kapasite inşası hedeflenmektedir. Bununla birlikte Balkanlar ve Avrupa'da organize suçlar kapsamında ele geçirilen elektronik delillerin mahkeme nezdinde anlamlı hale gelmesine fayda sağlayacak uygulamaların hayata geçirilmesi sağlanmaktadır. Son olarak organize suçlara ilişkin mali soruşturmaların siber suç soruşturmalarına entegre edilmesine yönelik ortak bir standart oluşturulmasına katkı sunulmaktadır. Söz konusu projelerin devamı niteliğinde olan CyberSEE projesinin Balkanlar ve Avrupa'da organize suçlara karşı geliştirilen siber suç stratejilerini konu aldığı görülmektedir. Öyle ki CyberSEE ile birlikte operasyonel olarak söz konusu stratejiler sahaya veya suç mahalline yansıtılabilmektedir. Bu kapsamda CyberSEE, hem siber suçlara hem de dijital delillere ilişkin önemli bir eylem planı hüviyeti kazanmıştır. Söz konusu eylem planında kritik altyapıların korunması hususuna da odaklanılmaktadır. CyberSEE projesi kamu-özel sektör arasında ortak iş birliği kapsamında siber dayanıklılığın güçlendirilmesi amacını taşımaktadır. En nihayetinde bahse konu projelerin Budapeşte Sözleşmesi'nin getirdiği temel ilkeler de göz önünde bulundurularak Balkanlar ve Avrupa'da yasal mevzuatın uyumlaştırılması ve uluslara-

rası adli yardımlaşma mekanizmalarının aktif hale getirilmesinde önemli bir rol üstlendiği değerlendirilmektedir.

Sonuç ve Değerlendirme

Bu çalışmada, tarih boyunca Balkanlar'ın stratejik ve jeopolitik konumu itibariyle geçiş hattında olması dolayısıyla siyasi nüfuz mücadelesine konu olduğu ortaya konulmuştur. Bu kapsamda yakın tarih boyunca yayılmacı devletlerin bölge ülkelerini kendi nüfuz alanlarına katma politikalarına makalede yer verilmiştir. Bununla beraber bölgede ortaya çıkan istikrarsızlık ve siyasi otorite boşluğu sebepli güvenlik sorunlarının baş gösterdiğine değinilerek organize suç ağlarının kara para aklama, kaçakçılık ve diğer yasa dışı faaliyetler yürüttüğüne vurgu yapılmıştır. Teknolojik gelişmelerle beraber konvansiyonel unsurlara entegre olan siber suç araçlarının sınır aşan hibrit tehdit tehlikesi oluşturduğu kanısına varılmıştır. Siber uzay bağlamında siber saldırı yöntemleri kullanılarak organize suç faillerinin anonim bir görünüşe kavuştuğu çıkarımı yapılmıştır. Çalışmada yer verilen uluslararası kuruluş raporları çerçevesinde bahse konu hibrit tehditlerle mücadelede siber saldırılara karşı yerel veya ulusal birimlerin yetersiz kaldığı, bu sebeple Avrupa Birliği ve Avrupa Konseyi öncülüğünde bölge ülkelerinin kolektif olarak müşterek bir savunma anlayışı içerisinde kapasite geliştirme projeleri geliştirmesi gerekliliği ortaya konulmuştur.

Son bölümde yer verilen projeler göstermektedir ki, Balkanlar coğrafi bağlamda Avrupa'ya uzanan arka kapı olması dolayısıyla stratejik olarak yeni güvenlik yaklaşımında devletler için önem arz etmektedir. Özellikle, Avrupa ve Asya arasında uyuşturucu maddelerin nakli, insan-silah kaçakçılığı ve kara para aklanması gibi organize suçlar bu coğrafi koridor üzerinden gerçekleştirilmektedir. Diğer taraftan bilgi ve iletişim teknolojilerinin gelişmesi ile birlikte siber suçların bölgede artış gösterdiği ve kaçakçılık girişimlerini kolaylaştırdığı çıkarımı yapılabilmektedir. Bölgede, tarihsel süreçte görülen yolsuzluklar, suçluların cezalandırılmasındaki noksanlık ve denetim eksikliği ile bölge ülkelerinin dijital altyapı alanında yetersiz olmasının siber saldırganların motivasyonunu artırdığı görülmektedir. Çalışmada yer verilen iPROCEED ve CyberSEE projeleri ile Güneydoğu Avrupa'da siber güvenlik ortamının geliştirilmesi, siber dayanıklılığın inşa edilmesi, bölge ülkelerine ait kritik altyapılar ve endüstriyel kontrol sistemlerinin güvenli hale getirilmesi hedeflenmektedir. Bununla birlikte yeni geliştirilen siber saldırı tekniklerine karşı müşterek bir savunma yaklaşımı ortaya konulmaktadır. 2016 yılından bu yana süregelen söz konusu projeler gelişen siber saldırılara uyarlanarak Balkanlar genelinde siber güvenlik stratejileri hayata geçirilmektedir. Söz konusu stratejilerde organize suçlar bağlamında suç gelirlerinin aklanmasının engellenmesi, dijital delil güvenliği, siber saldırıların önlenmesi ve siber dayanıklılık kapasitesinin artırılması amaçlanmaktadır. Bu hedefler doğrultusunda söz

konusu projelerin Balkanlar-Avrupa entegrasyonu çerçevesinde uyum süreçlerini destekleyeceği, siber kapasite inşasını geliştireceği ve Balkanlar'ın siyasi istikrarında belirleyici rol oynayacağı düşünülmektedir.

Bundan sonraki süreçte organizasyonel olarak siber suçlarla mücadelede yeni projelerin geliştirilmesi ve adli yardımlaşmanın güçlendirilmesi gerektiği değerlendirilmektedir. Europol bünyesinde faaliyet gösteren Ortak Siber Suç Eylem Görev Gücü (J-CAT) yapısına benzer olarak 7/24 çalışma esaslı bilgi paylaşımı yapacak bir platformun Balkanlar özelinde de hayata geçirilmesi önerilmektedir. Bununla birlikte makalede yer verilen raporlardaki istatistikler göz önüne alındığında, finans sektöründe gerçekleştirilen siber saldırılarda şüpheli finansal işlemlerin siber güvenlik birimlerine derhal bildirilmesini sağlayacak mekanizmaların desteklenmesi gerektiği düşünülmektedir. Bu kapsamda şüpheli işlemden etkilenen bölge ülkelerine yönelik yapay zekâ destekli erken uyarı sistemleri kurulması önerilmektedir. Diğer taraftan, kara para aklamanın bölgede özellikle kripto para birimleriyle gerçekleştirildiği görüldüğünden blokzincir (blockchain) üzerindeki anonim yasa dışı işlemleri tespit edecek yazılımların hayata geçirilmesi gerektiği değerlendirilmektedir. Buna yönelik inşa edilecek adli bilişim laboratuvarları aracılığıyla soğuk cüzdan analizi yapabilecek sistemlerin devreye alınması gerektiği düşünülmektedir. En nihayetinde Balkan ülkelerinin kritik altyapı sistemlerini korumak amacıyla olası siber saldırı senaryolarının tespit edildiği bölgesel tatbikat çalışmaları önerilmektedir.

Kaynakça

Anastasijevic, D. (2005). *Organized crime in the Western Balkans.* HUMSEC Project. https://www.files.ethz.ch/isn/102340/1_Anastasijevic.pdf

Andreas, P. (2011). *Criminalized conflict*: *The clandestine political economy of war and peace in the Balkans* (East European Studies Meeting Report No. 261). Wilson Center. https://www.wilsoncenter.org/publication/261-criminalized-conflict-the-clandestine-political-economy-war-and-peace-the-balkans

Asboth, E. T. (2025). *Transnational and transatlantic perspectives on the Balkans, 1850-1918: Historical Balkan narratives supported by Felix Philipp Kanitz, Mary Edith Durham, and Mihailo Pupin in the transnational public sphere*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-69180-5

Beraia, E. (2021). Hybrid warfare: NATO and the future of European and Asian security. In *Advances in military textbooks* (s. 45-60). IGI Global. https://doi.org/10.4018/978-1-7998-7118-7.ch003

Buçaj, E., Qehaja, D., Hoti, A., & Gara, A. (2025). Impact of socioeconomic factors on the proliferation of organized crime in Western Balkan countries. *Ekonomski Pregled*, 76(5), 372-388.

Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). (2012). *Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction*. Council of Europe.

Council of Europe, Cybercrime Convention Committee (T-CY). (2020). *The Budapest Convention on Cybercrime: Benefits and impact in practice* (T-CY(2020)16). Council of Europe.

Council of Europe, Cybercrime Programme Office (C-PROC). (2019). *iPROCEEDS: Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey* (Version 20 February 2019). Council of Europe.

Council of Europe, Cybercrime Programme Office (C-PROC). (2022). *Project of the European Union and the Council of Europe on targeting crime proceeds on the Internet and securing electronic evidence in South East Europe and Türkiye* (iPROCEEDS-2 summary). Council of Europe.

Council of Europe, Cybercrime Programme Office (C-PROC). (2024). *Project on enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye* (CYBERSEE summary). Council of Europe.

Council of Europe. (2024). *Declaration on strategic priorities for cooperation against cybercrime for South-East Europe and Türkiye*. Council of Europe.

Djokic, A. (2020). The perspectives of Russia's soft power in the Western Balkans region. *RUDN Journal of Political Science*, 22(2), 231-244. https://doi.org/10.22363/2313-1438-2020-22-2-231-244

Europen Union Agency for Cybersecurity (ENISA). (2025). *ENISA Threat Landscape 2025.* Publications Office of the European Union.

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Publications Office of the European Union.

Europol. (2025). *Steal, deal and repeat-How cybercriminals trade and exploit your data-Internet Organised Crime Threat Assessment (IOCTA) 2025*. Publications Office of the European Union.

Garčević, V. (2021). *The European Union dilemma: Russia's and China's increasing influence in the Western Balkans*. Boston University, Frederick S. Pardee School of Global Studies. https://open.bu.edu/handle/2144/44060

Huntington, S. P. (1996). *The clash of civilizations and the remaking of world order*. Simon & Schuster. s. 160-161.

Hupchick, D. P. (2002). *The Balkans: From Constantinople to Communism*. Palgrave Macmillan.

Jelavich, B. (1983a). *The history of the Balkans: Volume 1- Eighteenth and nineteenth centuries*. Cambridge University Press.

Jelavich, B. (1983b). *The history of the Balkans: Volume 2- Twentieth century*. Cambridge University Press.

Marleku, A., & Aliu, D. (2023). Russian influence on the European integration process of the Western Balkan countries: A comparative analysis. *Revista UNISCI*, (62), 183-203.

Marshall, T. (2015). *Prisoners of geography: Ten maps that explain everything about the world*. Scribner.

Rupnik, J. (Ed.). (2011*). The Western Balkans and the EU: 'The hour of Europe' (Chaillot Paper No. 126)*. European Union Institute for Security Studies.

Svetoka, S., & Doncheva, T. (2021). *Russia's footprint in the Western Balkan information environment: Susceptibility to Russian influence*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/russias-footprint-in-the-western-balkan-information-environment/216

Vezenkov, A. (2006). History against Geography: Should We Always Think of the Balkans as Part of Europe? In A. MacLachlan & I. Torsen (Eds.), *History and judgment* (IWM Junior Visiting Fellows' Conferences, Cilt 21).

Vucinich, W. S. (1965). *The Ottoman Empire: Its record and legacy*. D. Van Nostrand Company, Inc.

Yağcı, B. (2023). Bilgi ve iletişim teknolojilerinin gelişmesiyle değişen siber suç tanımı ve yaklaşımlar. *Bilgi Teknolojileri ve İletişim Dergisi*, 1(1), 147-182.

Zhilla, F. (2024). Decrypting the Balkan underworld: A theoretical analysis of encrypted communication in organized crime. *Jus & Justicia*, 18(1), 7-22. https://doi.org/10.58944/bgjy9350