



iPROCEEDS

Güneydoğu Avrupa ve Türkiye'de İnternet Üzerinden Elde Edilen Suç Gelirlerinin Önlenmesi Projesi

www.coe.int/cybercrime

21 Aralık 2017 tarihli versiyon

Yargıçlar ve Savcılara Yönelik Mesleki Eğitim

İnternet Kaynaklı Suç Gelirlerinin Aranması, Zapt Edilmesi ve Müsaderesi Hakkında İleri Seviye Eğitim

Kendi Kendine Eğitim El Kitabı

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

İletişim için:

Alexander Seger
Avrupa Konseyi
İnsan Hakları ve Hukukun Üstünlüğü Genel
Müdürlüğü
Siber Suçlar Bölümü
Strazburg, Fransa

Tel: +33-3-9021-4506
Faks: +33-3-9021-5650
e-posta: alexander.seger@coe.int

Sorumluluk Reddi:

Bu teknik rapor Avrupa Konseyi'nin ya da bu projeyi finanse eden hibe sağlayıcısının resmi pozisyonlarını yansıtmak zorunda değildir.

İçindekiler

1 Giriş	6
1.1 Eğitim Amacı	8
1.2 Hedeflenen Öğrenci Grubu	8
1.3 İçerik Özeti	9
1.3.1 İnternet Soruşturamalarında Güçlükler	9
1.3.2 Sınır Ötesi Soruşturamalar	9
1.3.3 Sanal Para Birimleri	9
1.3.4 Pratik Çalışma / Vaka Çalışmaları	9
2 İnternet Soruşturamalarında Güçlükler	10
2.1 Tipolojiler ve İnternet Üzerinde Kara Para Aklama	10
2.1.1 İnternet Bankacılığının Kullanılması	10
2.1.2 Diğer Finansal İnternet Hizmetlerinin Kullanılması	11
2.1.3 İnternet İletişim Hizmetlerinin Kullanılması	13
2.1.4 Kurşungeçirmez Barındırma	15
2.1.5 Yeraltı Ekonomisi	15
2.2 Fail Kimliğinin Saptanması	17
2.2.1 Ağ Adresi Çevirisi (NAT)	17
2.2.2 Taşıyıcı Ölçeğinde Ağ Adresi Çevirisi (CGN)	19
2.2.3 İP Numarasını Gizleyen (Anonimleştiren) Yazılımların Kullanılması	20
2.2.4 Çok Sayıda Bilgisayarın bir İP'ye Saldırması / Kötü Amaçlı Yazılımlar / Bir Bilgisayarın Uzaktan Kumanda Edilmesi	23
2.2.5 Açık, Kamusal ya da Çalıntı Kablosuz Bağlantı Kullanılması	23
2.2.6 Bir İP Adresi Sahibinin Kimliğinin Saptanması	24
2.3 İSS'ler ile İlişkiler	25
2.3.1 Talep Edilen Verilerin Türü	25
2.3.2 Avrupa Birliği Adalet Mahkemesi Kararı ile Geçersiz İlan Edilen AB Veri Saklama Direktifi	27
2.3.3 Ulusal İSS'ler	29
2.4 Çok Uluslu Hizmet Sağlayıcıları	30
2.4.1 Yargı Yetkisi	31
2.4.2 Genel Durum	31
2.4.3 Muhafaza Talepleri	31
2.4.4 Fevkalade Hal Talepleri	32
2.4.5 Talep Kapsamı	32
2.4.6 Talep Konusunun Bildirilmesi	32
3 Mali Soruşturamalar	34
3.1 Giriş	34
3.2 Mali Soruşturamalar ve İnternet Suç Gelirleri	34

3.2.1	Mali Soruşturma Unsurları	35
3.2.2	Mali Soruşturmanın Siber Suç ile ilgili Yönleri	35
3.2.3	Avrupa Birliği'nde Mali Soruşturma	36
4	Sınır Ötesi İşbirliği.....	38
4.1	Özet.....	38
4.1.1	Bilgi Alışverişine ve Hukuki Yardımlaşmaya Yönelik İlgili Ağlar ve Örgütler	39
4.1.2	Uluslararası Hukuki Araçlar	40
4.1.3	Uluslararası İşbirliği Hükümleri	42
4.2	Uluslararası İşbirliği Hükümlerinin Uygulanması Hakkında Değerlendirmeler	45
4.2.1	Suç Gelirlerinin Hedef Alınması Hakkında Değerlendirme	45
4.2.2	Siber Suç Hakkında Değerlendirme	47
4.3	Hukuki Yardımlaşmaya Yönelik Şablon ve Formların Kullanımı	55
5	Sanal Para Birimleri	57
5.1	Temel Eğitim Tekrarı	57
5.2	Sanal Para Birimlerine Giriş	58
5.2.1	Daha Fazla Sanal para Birimi Terminolojisi.....	58
5.2.2	Sanal Para Birimi Katılımcıları.....	60
5.2.3	Bitcoin	61
5.3	Sanal Para Birimi Riskleri	63
5.4	Soruşturmadaki Güçlükler	65
5.4.1	Sanal Para Birimlerinin Kullanılmış Olduğunu Bilmek	65
5.4.2	İşlemlerin Anonimliği	65
5.4.3	Kaynakların Kaynağı için Kimlik Saptama.....	66
5.4.4	Gelirlerin Nakde Çevrilmesi / Tahakkuku ve Tahvili	66
5.5	Dondurma/ Zapt Etme Konusundaki Güçlükler.....	67
5.5.1	Suç Gelirleri Olarak Sanal Para Birimleri	67
5.5.2	Sanal Para Biriminin Varlığının Saptanması	67
5.5.3	Sanal Para Biriminin Dondurulması / Denetiminin Ele Geçirilmesi.....	67
5.5.4	Varlık Yönetimi	68
6	Pratik Çalışma / Vaka Çalışmaları	70
6.1	Literatür Taraması	70
6.2	Vaka çalışması 1: Önlemin Hukuki Temeli Üzerine Düşünme.....	70
6.3	Vaka çalışması 2: Mali İstihbarat Birimi / Kolluk Kuvvetleri Etkileşimi Üzerine Düşünme.....	73
6.4	Vaka çalışması 3: Siber Suç / Kara Para Aklama Etkileşimi Üzerine Düşünme ...	76
7	Ek: İlgili Okumalar Listesi	78
7.1	Avrupa Konseyi	78
7.2	Avrupa Birliği	80
7.3	Birleşmiş Milletler.....	82

7.4	Mali Eylem Görev Gücü.....	83
7.5	İçtihat	83
7.6	Diğer referanslar.....	84

1 Giriş

Siber suç, elektronik kanıtlar, suç gelirleri ve kara para aklama konuları; farklı kurumları kesmekte ve özel olarak da siber suç birimlerini, mali soruşturma birimlerini, Mali İstihbarat Birimlerini (MİB'ler) ve kovuşturma hizmetlerini ilgilendirmektedir. Ancak, siber suç soruşturmalarına nadiren mali soruşturmalar, tersinden de mali veya diğer ceza soruşturmalarına nadiren siber suç soruşturmaları eşlik etmektedir. Bu bakımdan tüm bu kurumlar arasında daha etkili bir kurumlar arası işbirliğine ihtiyaç duyulmaktadır ve söz konusu işbirliğinin internet kaynaklı suç gelirlerinin aranması, zapt edilmesi ve müsaderesi üzerinde en güçlü şekilde etkiye bulunması beklenmektedir.

Siber suç ve internet üzerinde suç oluşturan para akışları coğrafi sınırlara takılmamaktadır. Dolayısıyla, bu olaylar kapsamlı bir biçimde ele alınmak isteniyorsa, soruşturma faaliyetleri sınırların ötesine doğru yayılmak ve aynı zamanda farklı yargı yetkisi alanlarında işletilmek zorundadır. Etkin uluslararası işbirliği; internet kaynaklı suç gelirlerinin aranması, zapt edilmesi ve müsaderesi açısından da çok önemlidir. Suç gelirleri izleme, kara para aklamayı önleme ve terör finansmanına karşı koyma tedbirlerini, siber suç ve adli bilişim ile alakalı soruşturmalarla bağlantılandırmak ek fırsatlar sunmaktadır. Örneğin, varlıkların dondurulmasına yönelik geçici tedbirlere elektronik kanıtların hızlandırılmış şekilde muhafaza edilmesi talebi eşlik etmelidir.¹ Mali Eylem Görev Gücü Tavsiye 36; başka nedenlerin arasında bir de bu nedenle, Budapeşte Siber Suçlar Sözleşmesi ile Avrupa Konseyi Varşova Sözleşmesi'nin uygulanmasını önermektedir.

Bilgi teknolojisinin kullanımı ve bilgi teknolojisine yönelik güven toplumda her geçen gün daha fazla yayıldıkça, bilgisayar sistemlerinin hedef alınması ve kötüye kullanımı da giderek daha yaygın hale gelmiştir. Bilgisayarları içeren suçlar hem sayıca hem de karmaşıklık düzeyi açısından hızla gelişmiştir, ancak etkin karşı önlemlerin geliştirilmesi konusunda geriden gelinmektedir. Saldırganların adalet karşısına çıkarılması makul şüphenin ötesinde suç kanıtı gerektirmektedir, ancak elektronik cihazlardan elde edilen kanıtlar uçucu olup çoğu zaman elle tutulur olmaktan uzaktır ve olasılıkla bir başka yargı yetkisi alanına girmektedir. Bu da elektronik kanıtların saptanması, toplanması ve muhafaza edilmesine yönelik etkin, hukuki açıdan uygun ve sağlam usullerin hayati öneme sahip olduğu anlamına gelmektedir. Ceza kovuşturmaları, giderek artan biçimde, siber suçlarla ya da bilgisayar sistemlerinde veya depolama cihazlarında bulunan elektronik kanıtlarla ilişkilenecek zorunda kalmaktadır.

Dünya genelinde toplumların bilgi ve iletişim teknolojilerine ne denli yüksek bir düzeyde yaslandığı düşünüldüğünde, hâkimlerin ve savcılarının siber suç ve elektronik kanıtlarla alakadar olmaya hazır hale gelmesi bir zorunluluk halini almaktadır. Pek çok ülkede kolluk kuvvetleri siber suçları araştırmak ve elektronik kanıtları korumak konusunda kapasitelerini kuvvetlendirebilmiş olsa da, hâkim ve savcılarının gereksinimlerine daha az odaklanılmıştır. Deneyim gösteriyor ki çoğu durumda hâkim ve savcılar siber dünyanın yeni gerçeklikleri ile başa çıkmakta zorluklarla karşılaşmaktadır. Dolayısıyla, hâkim ve savcılarının eğitim, ağ geliştirme ve uzmanlaşma yoluyla siber suçları hükme bağlamayabilmesini ve elektronik kanıtlardan yararlanabilmesini sağlamak için özel çabalar gerekmektedir.

¹ Bkz. paragraf 317, İnternet üzerinde suç oluşturan para akışları: yöntemler, eğilimler ve çok paydaşlı karşı koyma, MONEYVAL Araştırma Raporu, Mart, 2012. Ulaştırmak için bkz.:

[http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL\(2013\)6_Reptyp_flows_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf)

2009'da çok paydaşlı bir çalışma grubu ve Lizbon kenti yargı eğitimi kurumları ile işbirliği içerisinde gerçekleştirilen Siber Suç Projesi kapsamında, Avrupa Konseyi tarafından, bu türden çabaları destekleyecek bir fikir geliştirilmiştir.

Fikrin amacı yargı eğitimi kurumlarının hâkim ve savcılara yönelik olarak siber suç ve elektronik kanıtlar konulu eğitim programları geliştirmesine yardımcı olmak ve bu eğitimleri normal başlangıç eğitimi ve hizmet içi eğitim ile birleştirmek.

Hâkim ve savcılara yönelik eğitim fikrindeki amaçlar şunlardır:

- Eğitim kurumlarının uluslararası standartlar temelinde, başlangıç ve hizmet içi düzeyde siber suç eğitimi verebilmesini sağlamak
- Mümkün olan en fazla sayıda geleceğin hâkim ve savcısı ile mesleğini icra etmekte olan hâkim ve savcılara siber suç ve elektronik kanıtlar konusunda temel bilgilerle donatmak
- Önemli sayıda hâkim ve savcılara ileri düzey eğitim vermek
- Hâkim ve savcılarının süregelen uzmanlaşmasını ve teknik eğitimini desteklemek
- Hâkim ve savcılar arasında ağ geliştirme yoluyla bilgilerin artırılmasına katkıda bulunmak
- Farklı eğitim girişimleri ve ağlarına erişimi kolaylaştırmak.

Bu bağlamda, Avrupa Birliği ve Avrupa Konseyi Ortak Bölgesel Projesi SiberSuç@IPA (Ceza Yargılamasında Bölgesel İşbirliği: Siber suçla mücadelede kapasitelerin kuvvetlendirilmesi) yoluyla, eğitim kurumları tarafından kullanılmak üzere, siber suç ve elektronik kanıtlar konulu eğitim materyalleri geliştirilmiştir.

Avrupa Birliği ve Avrupa Konseyi Ortak Projesi iPROCEEDS² üzerinden siber suç ve elektronik kanıtlar konusunda hâkim ve savcılara yönelik temel ve ileri eğitimin yakaladığı başarı ve bu eğitimlerin ispatlanmış değeri göz önünde bulundurulduğunda, iki ek eğitim modülü geliştirilmiştir: internet kaynaklı suç gelirlerinin oluşturulması, aranması, zapt edilmesi ve müsadere konusunda bir temel ve bir ileri modül.

Genel olarak, suçluların ve suç örgütlerinin faaliyetleri kar yaratacak şekilde tasarlanmıştır. Birleşmiş Milletler tahminlerine göre 2009 yılında suç gelirlerinin toplam miktarı 2,1 trilyon Amerikan Doları olup bu da küresel GSYİH'nın % 3,6'sına denk düşmektedir; ancak bu kaynakların yalnızca çok küçük bir bölümü şimdiye dek kurtarılabilmektedir³. Ceza soruşturması ile paralel biçimde mali bir soruşturma yürütülmesi yoluyla suç gelirlerinin hedef alınması aynı zamanda kara para aklama suçuna dair kanıtları da açığa çıkarabilmektedir. Kara para aklama, suç örgütlerinin yasadışı faaliyetlerinden yarar sağlamalarını ve işlerini sürdürmelerini sağlamaktadır.

Siber suçların mali etkisini ve ilgili gelirlerin büyüklüğünü ölçmek güvenilir veri ve araştırmaların yokluğunda güç olmakla birlikte, vakalar göstermektedir ki siber suçlardan elden edilen gelirler hem geleneksel hem de yeni ödeme yöntemlerini içeren karmaşık düzenler üzerinden aklanmaktadır⁴. Ancak, siber suç soruşturmalarına nadiren mali soruşturmalar ve tersinden mali soruşturmalar veya diğer ceza soruşturmalarına nadiren siber suç soruşturmaları eşlik etmektedir.

Örgütlü suç grupları, varlıkları, onları yaratan suçun işlendiği devletten başka devletlerde saklanmakta ve yeniden yatırıma dökmektedir. Bu da yetkili makamların ciddi ve örgütlü

²Avrupa Birliği ve Avrupa Konseyi Ortak Projesi "Güneydoğu Avrupa ve Türkiye'de internet kaynaklı suç gelirlerinin hedef alınması" – iGELİRLER; Avrupa Birliği'ne Katılım Öncesi Mali Yardım Aracı bölgesindeki yetkililerin, siber suç gelirlerinin aranması, zapt edilmesi ve müsadere konusundaki kapasitesini kuvvetlendirmeyi ve internet üzerindeki kara para aklamayı önlemeyi amaçlamaktadır. <http://www.coe.int/en/web/cybercrime/iproceeds>

³Ceza hukuku ile kara para aklamayla mücadele edilmesi konulu bir AB Direktifi Önerisi'ne açıklayıcı not (22.12.2016). Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0826>

⁴İnternet üzerinde suç oluşturan para akışları: yöntemler, eğilimler ve çok paydaşlı karşı koyma, MONEYVAL Araştırma Raporu, Mart, 2012.

sınır ötesi suçla mücadele etmesini çok daha karmaşık hale getirmektedir. Aynı şekilde, siber suç ve internet üzerinde suç oluşturan para akışları coğrafi sınırları tanımamaktadır. Bu olayı kapsamlı bir biçimde ele almak için soruşturma faaliyetleri sınırları aşacak şekilde genişletilmeli ve aynı zamanda farklı yargı yetkisi alanlarında işletilmelidir. Bu nedenle, etkin uluslararası işbirliği de suç gelirlerinin aranması, zapt edilmesi ve müsaderesi açısından son derece önemlidir.

Bu mesleki eğitimde sunulan internet kaynaklı suç gelirlerini hedef alma fikri; hem suçlunun kovuşturulması hem de suç gelirlerinin hedef alınması bakış açısıyla, ceza soruşturmaları ile ceza kovuşturmalarının verimliliğini ve başarısını artırmak amacıyla, siber suç soruşturmaları, mali soruşturmalar ve kara para aklama soruşturmalarına ilişkin yaklaşımları bir araya getirmektedir.

1.1 Eğitimin Amacı

Bu eğitim; internet kaynaklı suç gelirlerinin soruşturulması, aranması, zapt edilmesi ve müsaderesi ile ilgili temel eğitimini tamamlamış olan ve bu alandaki eğitimine devam etmek isteyen ilgili hâkim veya savcının süregelen eğitimini kolaylaştırmak amacını taşımaktadır. Burada amaç; ilgili hâkim veya savcının yasal ve teknik düzenlemelerle alakalı bilgilerini, söz konusu bilgiler internet kaynaklı suç gelirleri ile alakalı olduğu ölçüde artırmaktır. Bu da; bu alanda seçilmiş bazı başlıkların daha detaylı bir biçimde incelenmesi sayesinde gerçekleştirilmektedir.

Eğitim, aşağıdaki alanlardaki seçili konuları daha detaylı bir biçimde inceleyecektir:

- İnternet üzerinde suç oluşturan para akışları ile alakalı yasal ve teknik soruşturma güçlükleri
- Sınır ötesi soruşturmaların uygulanabilirliği
- Sanal para birimlerinin suç oluşturacak biçimde kullanılması ve sanal para birimleriyle bağlantılı riskler

Ardından literatür taraması biçimde pratik çalışma ve öğrencinin üzerine düşüneceği vaka çalışmaları gerçekleştirilecektir.

1.2 Hedeflenen Öğrenci Grubu

Bu eğitim; hâlihazırda internet kaynaklı suç gelirlerinin soruşturulması, aranması, zapt edilmesi ve müsaderesi ile ilgili temel eğitimini tamamlamış olan hâkim ve savcılar için tasarlanmıştır. Bu el kitabının kullanıcılarının aşağıdakileri hâlihazırda bildikleri varsayılmaktadır:

- Siber suçun anlamı ve bir siber suç soruşturmasının niteliği
- Mali soruşturmaların niteliği
- Kara para aklama suçu ve Mali İstihbarat Birimi'nin (MİB) rolü
- İP adresinin niteliği türünden temel teknik bilgiler
- Elektronik kanıtların özelliklerine dair temel anlayış

Tüm bu ön şartlar Avrupa Konseyi'nin "İnternet Suç Gelirlerinin Aranması, Zapt Edilmesi ve Müsaderesi Konulu Temel Eğitim"i'nin tamamlanması yoluyla karşılanabilir.

1.3 İçerik Özeti

1.3.1 İnternet Soruşturmalarda Güçlükler

Temel derste, internet üzerinde suç oluşturan bir dizi para akışı ve kara para aklama tipolojisi tanıtılmıştır. Bu bölümün amacı; orada tanımlanan tipolojilerden bir seçki ile deneyimlenebilecek soruşturma güçlüklerinden bazılarını daha detaylı bir biçimde tartışmaktır. Bu da internet üzerindeki bir failin saptanması, internet kaynaklı suç gelirlerinin saptanması ile bağlantılı, aynı zamanda ulusal, uluslararası ve çok uluslu İnternet Servis Sağlayıcıları (İSS'ler) ile ilişkilerle alakalı güçlükleri konu alan bir tartışmayı içermektedir.

1.3.2 Sınır Ötesi Soruşturmalar

İnternet kaynaklı suç gelirlerinin hedef alınması fikri; hem suçlunun kovuşturulması hem de suç gelirlerinin hedef alınması bakış açısıyla, ceza soruşturmaları ile ceza kovuşturmalarının verimliliğini ve başarısını artırmak amacıyla, siber suç soruşturmaları, mali soruşturmalar ve kara para aklama soruşturmalarına ilişkin yaklaşımları bir araya getirmektedir.

Yurtdışında mahkeme kararlarının uygulanmasında ve kanıt toplanmasında hukuki yardımlaşma hala başlıca araç olarak görülmekte ise de, prosedür uzunluğu önemli bir engel oluşturmaktadır. Ancak, ortak soruşturmaların ve ortak soruşturma ekiplerinin kullanılması bazı verimlilik sorunlarına çözüm olabilmektedir. Kolluk kuvvetleri (polis ve savcılar) alanındaki işbirliği ve bilgi alışverişi sınır ötesi vakaların ayrılmaz unsurudur. İlgili ağlar bu bakımdan önemli bir rol oynamaktadır.

Bu ileri eğitimin amaçları bakımından, uluslararası örgütlerce saptanmış, ulusal mevzuat ve uygulamada uluslararası standartlara başvurulması önündeki engellere ilişkin son dönem bulgularından kimilerini, ayrıca bir esin kaynağı olarak kullanılabilecek ilgili tavsiyeleri vurgulamak yararlı olacaktır.

1.3.3 Sanal Para Birimleri

Giriş eğitiminde tartışılmış olan sanal para birimleri ile alakalı temel terminolojiden devam ederek, bu eğitim, sanal para birimi takasları, cüzdan hizmetleri vs. de dâhil olmak üzere sanal para birimi ekosistemindeki katılımcılar hakkında daha fazla ayrıntı sunmaktadır. Bitcoin sanal para biriminin işleyişi anlatılmakta ve ardından sanal para birimi kullanımını içeren soruşturmalarla bağlantılı riskler ve meydan okumalar, aynı zamanda bunların aranması, zapt edilmesi ve varlık yönetimine tabi tutulması konuları açıklanmaktadır.

1.3.4 Pratik Çalışma / Vaka Çalışmaları

Bu eğitimde sağlanan bilgileri kendi ulusal mevzuatlarına oturtmak konusunda öğrencilere yardım etmek üzere, öğrencilerin, burada gündeme getirilen konuları daha ileri düzeyde araştırabilmesi için, rehberli bir literatür taraması ve bazı vaka çalışmaları verilmektedir.

2 İnternet Soruşturmalarda Güçlükler

2.1 Tipolojiler ve İnternet Üzerinde Kara Para Aklama

Temel derste, internet üzerinde suç oluşturan bir dizi para akışı ve kara para aklama tipolojisi tanıtılmıştır. Bu bölümün amacı; orada tanımlanan tipolojilerden bir seçki ile deneyimlenebilecek soruşturma güçlüklerinden bazılarını daha detaylı bir biçimde tartışmaktır. Bu eğitimde kendi bölümleri çerçevesinde ayrı ayrı tartışılacak, çok büyük ve yaygın şekilde karşılaşılan iki mesele bulunmaktadır; internet üzerindeki bir failin saptanması ile bağlantılı soruşturma güçlükleri (bkz. Bölüm 2.2) ile sanal para birimlerinin kullanımıyla ilişkili çok sayıda güçlük (bkz. Bölüm **Error! Reference source not found.**).

2.1.1 İnternet Bankacılığının Kullanılması

Temel eğitimde tartışılmış olan tipolojilerden bazıları bir banka hesabına erişimi olan suçluya dayanmaktadır. Özel olarak da banka havaleleri, banka hesabı devralmaları ve uluslararası havaleler ile ilgilidir. Müşterilere karşı gerekli özen, kayıtların tutulması vs. açısından mali kurumlar üzerindeki düzenleyici şartlar iyi anlaşılmaktadır⁵. Ancak suçlular, bu türden kontrolleri baypas etme girişimlerinde, internet bankacılığı ortamının yüz yüze olmayan niteliğine yaslanmaktadır⁶. Örneğin bir suçlunun, doğrudan müşteri temasına ihtiyaç duyulmaksızın (örneğin, internet bankacılığı kimlik bilgilerini çalarak ya da kullanarak) meşru bir bankacılık müşterisinin kimliğine bürünmesi mümkündür ve bu bir mali kurumun tespit etmesi açısından çok daha büyük bir zorluk içermektedir.

Bu türden davaları soruştururken izlenecek başlıca üç yol bulunmaktadır:

- Banka hesabının tehlikeye girme biçimi (örneğin, şifre avcılığı, kötü amaçlı yazılım bulaştırılması). Bu konuda kanıtlar büyük bir ihtimalle mağdur olan hesap sahibinden edinilebilir.
- Tehlikeye giren banka hesabının oturum açma bilgileri. Bu bilgi mali kurum tarafından sağlanabilir.
- Tehlikeye giren hesaptan para havale etmek için kullanılan banka hesabı/hesapları. Bu bilgi mali kurumun elinde olup sürece dâhil olan bireylerin (para kuryelerinin) saptanması ve nihai zapt etme için paranın izlenmesinde yardımcı olabilir.

Bu bölümün geri kalanında, internet bankacılık hizmetlerinin kullanımı nedeniyle daha karmaşık hale gelmiş olan belirli soruşturma konuları tartışılacaktır.

İlk olarak, hesap sahibi ile şüpheli arasında bir ilişki varsa, bu ilişkinin niteliğini belirlemek daha güçtür. Örneğin:

1. Banka hesabının sahibi şüphelinin faaliyetinden haberdar mıdır?
2. Şüphelinin banka hesabı üzerinde dolaysız kontrolü var mı, yoksa şüpheli banka hesabı sahibinin faaliyetlerini mi yönlendirmekte?

⁵Kara Para Aklama, Terörizmin Finanse Edilmesi ve Silahlanma ile Mücadelede Uluslararası Standartlar, Mali Eylem Görev Gücü (MEGG) Tavsiyeleri, 2012. Ulaşmak için bkz.:

<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

⁶MEGG Raporu, Yeni Ödeme Yöntemleri Kullanarak Kara Para Aklama, Ekim 2010. Ulaşmak için bkz.: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

3. Hesap üzerinde belirli bir işlemi gerçekleştiren kişiyi saptamak mümkün müdür? Bu ve diğer pek çok sorunun ortaya koyduğu gibi, internet bankacılık ortamının yüz yüze olmayan niteliği bir soruşturmada gerçeklerin tespitini güçleştirmektedir.

İkincisi, internet bankacılık hizmetlerinin kullanımı, şüpheli faaliyetin kendisinin saptanması bakımından da bazı güçlükler yaratmaktadır. Bir şubede, bir şüpheli kendisini tanıtip işlem yapmaya çalıştığında, veznedarın gerçekleştirilmekte olan faaliyetin açıkça şüpheli olup olmadığını saptamak konusunda en azından bir şansı vardır. İnternet ortamında işlemler büyük oranda otomatikleştirilmiştir. Raporlama sınırlamalarından kaçınmak üzere fonların yapılandırılması eğilimiyle birleştiğinde, bu durum, şüpheli işlemlerin kaçırılabilmesi riskinin artması sonucunu doğurabilmektedir. Bununla mücadele etmek için, mali kurumlar çoğu zaman otomatikleştirilmiş işlem izleme yazılımları kullanmaktadır; bu yazılımların işlevi belirli bir hesap üzerinde genellikle gerçekleştirilen işlemlerin profilinden sapan işlemleri saptamaktır.

Hepsi olmasa da bazı dolandırıcılık izleme yazılımları, bir internet bankacılık hesabında oturum açılırken kullanılan İP adresini de kontrol edecektir. Eğer, örneğin, İP adresi hesabın daha önce hiç oturum açmadığı bir adres ise, bu durum, internet bankacılık hesabının gizliliğinin ihlal edilmiş olabileceği şüphesini gündeme getirmekte kullanılabilmektedir. Ancak, mali kurumların uygulamaya ilişkin bakış açısıyla düşünüldüğünde, dolandırıcılığı saptamak ve önlemek ile küresel olarak hareketli müşterilerin meşru bankacılık faaliyetlerini engellemek arasında ustalık ve dikkat isteyen bir denge söz konusudur.

Ayrıca, bir müşterinin internet bankacılığı hesabının gizliliği ihlal edilmiş olsa bile, bu durum oturum açmak için kullanılan İP adresinden her zaman için görünür olmayacaktır. Bunun nedeni; müşteri bilgisayarına kötü amaçlı bir yazılım bulaşmış olması halinde, suçlunun müşteri bilgisayarını üzerinde kontrol edinmesinin mümkün hale gelmesidir. Bu sayede suçlu, müşterinin bilgisayarının İP adresinden müşteri hesabında oturum açma işlemi gerçekleştirebilir, dolayısıyla beklenmedik bir İP adresinden yapılan oturum açma işlemi nedeniyle açığa çıkacak uyarının tetiklenmesini önleyecektir.

Üçüncüsü, şüphelinin faaliyetlerini ispatlamak için hangi ek kanıtlara gereksinim duyulduğu ve bu kanıtların erişilebilir olup olmadığı meselesi söz konusudur. Belirli bir hesap için oturum açma işlemi yapılan İP adresleri mali kurum tarafından büyük bir olasılıkla kayıt edilmiş olacaktır, ancak bu kayıtlar her zaman kolaylıkla erişilebilir olmayacaktır. Hangi hesaplar tarafından hangi oturum açma işlemleri için hangi İP adreslerinin kullanıldığını saptamak ciddi çaba gerektirebilir. Bunun nedeni internet bankacılığı altyapısının karmaşıklık düzeyi ile özel olarak da sistem günlüklerinin gerekli bilgilere kolay erişim sağlanacak bir biçimde depolanamaması ya da ilişkilendirilememesidir. Ek olarak, şüpheliyi söz konusu İP adresi ile bağlantılandırmak suretiyle, kullanılmış olan İP adresinin saptanıp saptanamayacağı ve ne zaman saptanabileceği güçlük içeren ayrı bir meseledir.

2.1.2 Diğer Finansal İnternet Hizmetlerinin Kullanılması

Diğer (bankacılık dışı) finansal internet hizmetleri, temel eğitimde tartışılan tipolojilerin birçoğunda rol oynamaktadır. Bu bakımdan, özel olarak da internet ödeme sistemleri, internet üzerinden yapılan satın almalar ve internet kumar/ticaret platformlarının kullanımından söz edilebilir. Bir kez daha, hizmet ile hizmetin kullanıcısı arasındaki ilişkinin yüz yüze olmayan niteliği suçlulara bu türden hizmetleri sömürme şansı tanımaktadır.

Nihayetinde bu hizmetler geleneksel finansal hizmetler sektörüyle bir etkileşim biçimine sahip olmak zorunda kalacaktır. Bunun en yaygın gerçekleşme biçimi, finansal internet

hizmetleri sağlayıcısı üzerinden bir hesabın “doldurulması” için kullanılan ödeme kartlarıdır. Bir ödeme kartından hizmet sağlayıcısına fon aktarıldıktan sonra, kullanıcı ile finansal internet hizmeti sağlayıcısı arasındaki takip eden etkileşimlerin niteliği geleneksel finansal sistem açısından opak hale gelmektedir. Dolayısıyla internet ödeme hizmetlerinin uygunluk yükümlülüklerine ve denetime tabi olması önerilmektedir⁷. Bu düzenlemenin niteliği bir yargı yetkisi alanından diğerine değişebilmektedir.

Örneğin, mikro ödemeler kavramını düşünün⁸. İnternet ödeme hizmetinin her bir mikro ödemeyi derhal kullanıcının kredi kartına borç kaydetmesi mali olarak anlamlı olmayacaktır; zira ödeme kartı ücretleri işlem gören ödeme hizmetine yönelik karı ortadan kaldıracaktır. Bunun yerine, ödeme hizmetleri tipik olarak belirli bir süre boyunca bir dizi ödemeyi bir araya getirmekte ve belirli bir süre için tüm kullanıcı faaliyeti için tek bir borç kaydetmektedir. Ödeme hizmeti bu nedenle bir miktar sahtecilik riskini kabul etmektedir ancak bireysel ödemeler kapsamına giren para miktarı tipik olarak çok düşük olduğundan, genel kayıplar küçük olma eğilimindedir.

Bir mikro ödeme modeli kimi zaman da cep telefonu operatörleri tarafından sunulmaktadır. Bu örneklerde, kullanıcı telefonunu veya telefon numarasını kullanarak mikro ödemeler yapmakta ve borç kayıtları kullanıcının bir sonraki telefon faturasına eklenmektedir.

Bu örneklerde, suç faaliyetini kanıtlamak ve para akışının izini sürmek bakımından soruşturma görevlisi için en önemlisi yasadışı faaliyetin niteliğini (dolandırma, yetkisiz erişim), toplanabilecek verilerin türlerini ve nereden toplanabileceğini açıklığa kavuşturmadır.

Örneklerin büyük bölümünde mağdurlar, banka hesaplarını veya kredi kartlarını ilgilendiren dolandırıcılıklarda daha geç bir aşamada uyarılmaktadır. Yine de, ödeme hizmetleri sağlayıcıları, yasadışı faaliyetleri saptayabilmekte ve verileri muhafaza edebilmekte, bunları daha sonra soruşturma görevlilerine sağlayabilmektedir.

İnternet ödeme hizmetlerinin kullanılması nedeniyle ortaya çıkan başlıca güçlük, gerekli kayıtların tipik olarak farklı bir yargı yetkisi alanında bulunması ile ilgilidir. Çok uluslu hizmet sağlayıcılarının ve hukuki yardımlaşma sürecinin devreye girmesi bir soruşturmayı kayda değer biçimde yavaşlatıp karmaşıklık düzeyini artırabilmektedir.

İnternet üzerinden yapılan satın almaları kolaylaştıran platformların kullanımı ile benzeri sorunlar ortaya çıkmaktadır. Temel eğitimde tartışıldığı üzere, internet üzerinden mal ve hizmetlerin satın alınması, ardından bunların suçluya veya kuryeye gönderilmesi; çalıntı ödeme bilgilerinin gerçek dünya değerine dönüştürülmesine iyi bir örnektir. Bu örneklerde, soruşturma bütünüyle satın alma platformunun kayıt tutmasına ve şüpheli faaliyetleri saptama becerilerine yaslanmaktadır. Burada da, soruşturmaların çoğunda, büyük internet satın alma platformlarının çoğunluğunun bir başka yargı yetkisi alanına girdiği görülecektir. Bu kuruluşlardan kanıt toplamak, söz konusu yargı yetkisi alanına bir hukuki yardımlaşma anlaşması talebi sunulmasını gerektirecektir.

İnternet kumar platformları da esas itibarıyla dünya genelinde bu kuruluşların birbirini tutmayan düzenlemelere tabi olması nedeniyle bazı benzersiz güçlükler ortaya çıkarmaktadır. Örneğin, bazı yargı yetkisi alanlarında internet kumarı yasadışıdır, dolayısıyla bu örneklerde bir internet kumar şirketi işletmecisi ile işbirliği yapmak bu kuruluşların tanındığına işaret edebilmekte ve bu nedenle hukuki güçlükler

⁷MEGG Raporu, Yeni Ödeme Yöntemleri Kullanarak Kara Para Aklama, Ekim 2010. Ulaşmak için bkz.: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20Using%20New%20Payment%20Methods.pdf>

⁸<https://en.wikipedia.org/wiki/Micropayment>

yaratabilmektedir. AB çerçevesinde, örneğin, 20 AB üyesi devlet internet kumarına izin verirken, yedisi vermemektedir. Bazıları, son dönemin mevzuatına binaen, internet kumarına izin vermeye ya da onu yasaklamaya karar vermişken, diğerleri geleneksel kumar için çoğu durumda yıllar önce oluşturulmuş olan mevzuatı uygulamaya devam ederek "edilgen biçimde" internet kumarına izin vermekte ya da onu yasaklamaktadır. İnternet kumarına izin veren yirmi Üye Devlet arasından on üçü serbest bir piyasa işletirken, altısı devletin sahip olduğu tekelleri çalıştırmaktadır ve biri de özel bir tekeli ruhsatlandırmıştır⁹.

2.1.3 İnternet İletişim Hizmetlerinin Kullanılması

İnternet eninde sonunda bir iletişim platformudur ve suçlular faaliyetlerini kolaylaştırmak amacıyla iletişim hizmetlerini kullanmaktadır. Özel olarak internet üzerinde suç oluşturan para akışları bağlamında, internet üzerindeki iletişim hizmetleri kurye bulmayı, iletişim ve yönetimi kolaylaştırmaktadır. İnternet üzerinden erişilebilir olan e-posta, internet bağlantılı sohbet, anlık mesajlaşma ve telefon gibi hizmetler suçlular tarafından faaliyetlerini örgütlemek üzere kullanılabilir.

Gerek bir iletişimin taraflarının gerekse içeriğinin saptanması açısından teknik zorluklar yaşanabilmektedir. İnternet üzerinden şüphelilerin kimliğinin saptanması meselesi Bölüm 2.2 çerçevesinde detaylı bir biçimde tartışılmaktadır.

Son yıllarda, internet hizmetleri sağlayıcıları arasında, kullanıcılarının mahremiyetinin güvence altına alınmasına yönelik artan bir odaklanma eğilimi olduğu görülmektedir. Bu eğilim, artan şifreleme kullanımında olduğu gibi, pek çok örnekte kendisini göstermektedir. Şifreleme kabaca üç farklı biçimde kullanılmaktadır¹⁰:

- **Tüm disk veya cihaz şifrelemesi:** Bir dizüstü bilgisayar veya kişisel bilgisayar örneğinde, sabit sürücünün tüm içeriğini şifrelemeye yönelik teknolojiler bir süredir mevcuttur. Bir süredir akıllı telefon gibi mobil bir cihazın hafızasını aynı şekilde şifrelemek de mümkün hale gelmiştir. 2014 dolaylarında, Apple ve Google gibi teknoloji şirketleri akıllı telefonlarında cihaz şifrelemesini fabrika ayarı olarak sunmaya başlamıştır. Şifreleme ve cihaza giriş tipik olarak bir parola veya PIN gerektirmektedir. Bu türden bir şifrelemenin arkasındaki meşru gereklilik akıllı telefon sahibinin kişisel verilerini cihazın kaybolması veya çalınmasına karşı korumaktır.
- **Uçtan uca şifreleme:** Bu ifade, bir mesajlaşma platformu üzerinden gönderilen mesajların yalnızca göndericisi ve alıcısı tarafından okunabilecek biçimde şifrelenmesi için kullanılmaktadır. iMessage, WhatsApp ve Facebook Messenger da dâhil olmak üzere pek çok mesajlaşma servisi mesajların uçtan uca şifrelenmesi konusunda çeşitli çözümler sunmaktadır. Örnek olarak iMessage ele alınırsa, uçtan uca şifrelemenin, hizmet sağlayıcısı olarak Apple şirketinin dahi mesajların içeriğine erişimi olmaması anlamına geldiği görülür.
- **Aktarım Şifrelemesi:** Bu şifreleme biçimi iki taraf arasındaki aktarım için şifrelenen verilere atıfta bulunmaktadır. Bu günlerde en yaygın biçimde, internet sayfası trafiğinin şifrelenmesine atıfta bulunmak için kullanılmaktadır. Aktarım şifrelemesi, herhangi bir saldırganın bir müşteri ile bir banka veya e-ticaret sitesi arasındaki iletişimde araya girmesini engelleyerek, modern e-

⁹Politika Departmanı tarafından hazırlanan AB Parlamentosu Çalışması, Ekonomik ve Bilimsel Politika, "İnternet Kumarı, bütünlük ve kumara yönelik bir yasa vurgusu". IP/A/IMCO/FWC/2006-186/C1/SC2. Ulaşmak için bkz.:

[http://www.europarl.europa.eu/RegData/etudes/etudes/JOIN/2008/408575/IPOL-IMCO_ET\(2008\)408575_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/JOIN/2008/408575/IPOL-IMCO_ET(2008)408575_EN.pdf)

¹⁰Bir İnsan Hakları Meselesi olarak Şifreleme, Uluslararası Af Örgütü Raporu, 2016 Marti. Ulaşmak için bkz.:

http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

ticaret ve e-bankacılık işlemlerini olanaklı kılan temel güvenlik kontrollerinden birisini oluşturmaktadır.

Aktarım şifrelemesi kullanımını içeren örneklerde, iletişimde araya girilmesi türünden özel soruşturma önlemleri, internet sitesi sahibi ve/veya İnternet Servis Sağlayıcısı gibi ilgili tarafların işbirliği ile teknik olarak yine de mümkün olabilmektedir. Şifrelenmiş bir cihaza veya uçtan uca şifreleme yoluyla şifrelenmiş bir iletişime erişim sağlamak daha güçtür ve çoğu zaman şüphelinin cihazına veya bilgisayarına erişim gerektirecektir.

VAKA ÇALIŞMASI: APPLE MI FBI MI¹¹

FBI; Aralık 2015'te 14 ölüme neden olan, Kaliforniya, San Bernardino'da yaşanan bir silahlı saldırının faillerinden birisi tarafından kullanılan bir iPhone 5C marka telefonun kilidini açmak istemiştir.

16 Şubat 2016'da, ABD Adalet Bakanlığı tarafından yapılan bir talebe cevaben, federal bir sulh hâkimi, Apple şirketinin, dava üzerinde çalışan dedektiflerin telefonun güvenlik özelliklerinin etrafından dolanmalarını sağlayacak özel bir İOS işletim sistemi versiyonu yaratması için emir çıkarmıştır. Apple Yönetim Kurulu Başkanı Tim Cook açık bir mektupla cevap vermiş ve bu mektupta hükümetin taleplerinin "tüyler ürpertici" sonuçları olan bir "mahremiyet ihlali" oluşturduğunu belirtmiştir. Cook şöyle demiştir:

"FBI bizim maliki olduğumuz bir şeyi istediğinde, onu sağladık. Apple geçerli celp ve arama emirlerine uydu, San Bernardino davasında da böyle oldu. Apple mühendislerinin FBI'ya tavsiyede bulunmalarını da sağladık ve erişimlerinde olan bir dizi soruşturma seçeneği hakkındaki fikirlerimizi de kendilerine sunduk... Ancak şu anda ABD hükümeti basitçe sahip olmadığımız ve yaratılmasının çok tehlikeli olduğunu düşündüğümüz bir şeyi istiyor bizden. Bizden iPhone'a arka kapıdan giriş inşa etmemizi istediler."

Apple mahkeme emrini temyize götürmüş ve 22 Mart 2016 tarihine bir federal duruşma konmuştur. Sayısız bağımsız teknoloji uzmanı, hukuk profesörü, teknoloji şirketleri ve insan hakları örgütleri Apple şirketinin bu meseledeki duruşunu desteklemiştir. Uluslararası Af Örgütü de dâhil olmak üzere FBI'nın talebine karşı çıkanlar arasında paylaşılan yaygın bir görüş şudur: eğer Apple bu telefonun kilidini kaldıracak şekilde yazılımını değiştirmeye zorlanırsa, ABD hükümetinin (ve potansiyel olarak diğer hükümetlerin) teknoloji şirketlerini istihbarat ve diğer güvenlik örgütlerine bir "arka kapı" sağlayarak şifreleme süreçlerini zayıflatmaya ya da bozmaya zorlayabilmesine bir emsal oluşturacaktır.

Davaya cevaben, BM İnsan Hakları Yüksek Komiserliği şu açıklamada bulunmuştur: "ABD'de Apple şirketine karşı kazanılacak bir dava, dünyanın herhangi bir yerinde Apple veya herhangi bir büyük uluslararası bilgi teknolojisi şirketinin müşterilerinin mahremiyetini savunmasını imkânsız hale getirebilecek bir emsal oluşturacaktır; suç ile ilişkili bilgisayar korsanları için olduğu kadar otoriter rejimler için de potansiyel bir hediyedir bu. Diğer devletlerdeki makamların, Google ve Blackberry gibi bilgi teknolojisi ve iletişim şirketlerini, müşterilerini kitlesel düzeyde izlemeye maruz bırakmaya zorlayacak bazı çok güçlü çabaları hâlihazırda olmuştur."

28 Mart günü, FBI üçüncü bir tarafın yardımıyla iPhone kilidini açtığını ifade etmiş ve Adalet Bakanlığı davayı geri çekmiştir.¹²

¹¹*Ibid.*

2.1.4 Kurşungeçirmez Barındırma

Pek çok internet ve ağ barındırma servisinin hizmet şartları, ağları ya da hizmetleri üzerinde yasadışı faaliyetlere müsaade etmemektedir. Dolayısıyla kolluk kuvvetlerinden gelen bilgi taleplerinde ve yasadışı alanlara ve internet sitelerine erişimin durdurulması konusunda genellikle işbirliği yapacaklardır.

Kurşungeçirmez barındırma ise kolluk kuvvetlerinden gelen bilgi ya da internet sitelerine erişimin durdurulması talepleriyle işbirliği yapmayan barındırma servislerine verilen isimdir. Çoğu zaman bu servisler (soruşturmanın devam ettiği ülkeye göre) coğrafi olarak başka ülkelerde yer almaktadır. Örneklerin çoğunda kurşungeçirmez barındırma şirketleri, altyapılarını kullanan müşterilerinin yürüttüğü suç faaliyetleri konusunda yasal sorumluluk taşımadıklarını ifade ederek kendilerini savunmaya çalışacaklardır.

Bu servisler sıklıkla yasadışı malzeme dağıtımında, istenmeyen e-posta yaratmak için, kötü amaçlı yazılımlar ve diğer suç altyapısı biçimleri için komuta ve kontrol sunucuları olarak kullanılmaktadır^{13, 14, 15}.

İnternet bankacılık hizmetlerinin (ve diğer internet hizmetlerinin) müşterilerini hedef alan, şifre avcılığı siteleri sıklıkla yasal internet sitelerine benzer görünen internet siteleri yaratmak için kurşungeçirmez barındırma kullanmaktadır. Bunlar çoğunlukla finansal kurum markasının izinsiz kullanımına dayanarak erişime kapatılmakta veya engellenmektedir. Yasal bir kuruluşun markasını kullanmayan internet sitelerine erişimin durdurulması daha zor olabilmektedir.

Bazı ülkelerdeki mevzuat, çeşitli teknik filtreleme yöntemleri kullanılarak, yasadışı olduğu bilinen içerikleri İSS'lerin engellenmesini desteklemektedir¹⁶.

Kurşungeçirmez barındırma şirketleri tarafından kullanıcıları ve hizmetleriyle ilgili olarak yetkililere sağlanan bilgiler, bir soruşturma sürecinde çok fazla işe yaramamaktadır zira bu bireylere ilişkin detaylar çoğu zaman sahtedir. Ancak, kiralanan hizmetler için kullanılan ödeme yöntemi bir suç faaliyetinin kaynağının saptanmasına yardımcı olabilecek önemli bir ipucu olabilmektedir.

Kanuni açıdan, gerçekleştirilen yasadışı faaliyetlere yönelik yargı yetkisi alanını belirlemekte de güçlükler vardır, çünkü birden fazla kaynak, hedef nokta veya diğer koordinasyon yerleri/kuruluşları söz konusu olabilmektedir.

Kurşungeçirmez barındırmanın bulunduğu ülkelerde, soruşturma sırasında iletişimde araya girme yöntemine başvurulabilmektedir. Bu, suç faaliyetinin kaynağı, hedefi ve niteliği konusunda bilgi toplanmasına yardımcı olacaktır.

2.1.5 Yeraltı Ekonomisi

¹²FBI Apple yardımcı olmaksızın teröristin iPhone'unu kırdığını söylüyor, CNN, 29 Mart 2016,

<http://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/index.html>

¹³<http://www.cio.com/article/2428317/infrastructure/in-china--700-puts-a-spammer-in-business.html>

¹⁴http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_2.html?sid=ST2008111801165&s_pos=

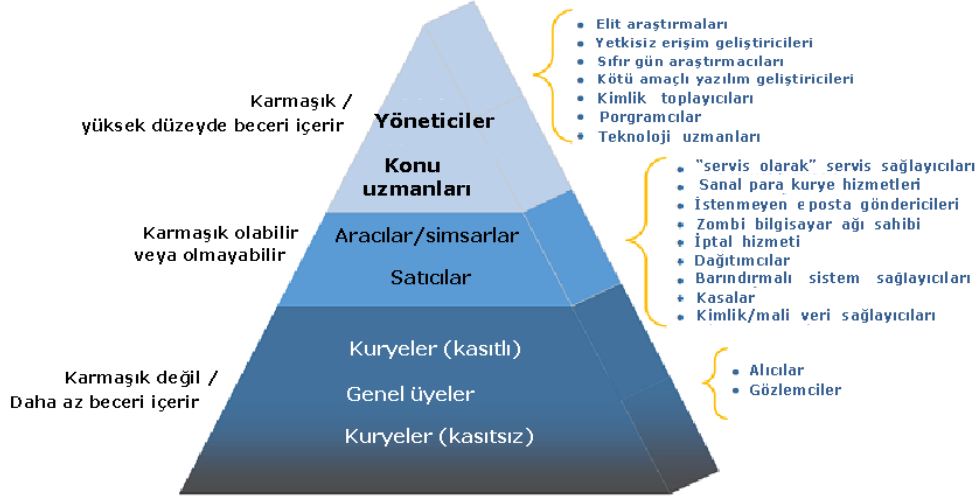
¹⁵https://en.wikipedia.org/wiki/Bulletproof_hosting

¹⁶T-CY(2006)04 Kolluk kuvvetleri ile özel sektör arasındaki işbirliğinin güçlendirilmesi, özel sektörün çocuk pornografisi sitelerini nasıl engellediğine dair örnekler, Şubat 2006. Ulaşmak için bkz.:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>

Yeraltı ekonomisi suçluların birbirleri ile hizmet ve bilgi alışverişinde bulunmak için kullandıkları hizmetlere verilen isimdir. İpek Yolu ve KaranlıkPiyasa (DarkMarket) gibi pek çok yeraltı forum örneği bulunmaktadır.¹⁷

Yeraltı ekonomisi örgütsel olarak suç işlemek üzere yapılandırılmıştır. Çoğu zaman Bir-Hizmet-Olarak-Suç adını taşıyan bir iş modeli kullanılmaktadır.



Şekil 1: Karanlık Ağda Suç Oluşturan İş Modeli Katılımcıları

Resim Empact eğitimi

Ağırlıklı olarak kredi kartı dolandırıcılığına ve çalıntı kredi kartı verilerinin satışına adanmış yeraltı forumları çoğu zaman kredi kartı ve banka bilgileri dolandırıcılık forumları olarak anılmaktadır.

Çoğu durumda bu forumlar şifre ya da başka güvenlik önlemleri kullanımı temelinde yalnızca sınırlı "müşteriler" için açıktır.

Bu türden forumların içine doğru genişleyen soruşturma süreçleri çoğu zaman çok uzun ve karmaşık olmakta, gizli ajanlar çoğu zaman bu forumların içine yavaş yavaş sızıp forum yöneticilerine ve işletimcilerine karşı suçlamaların yapılabilmesini sağlayacak şekilde bilgilere erişim sağlayacakları yetki pozisyonlarına ilerlemektedirler. Bu türden karmaşık soruşturma süreçlerinin gerekliliği şu anlama gelmektedir; çoğu soruşturmada tekil bir internet suç eylemi ya da kara para aklama soruşturması için kanıt toplamak üzere bir yeraltı forumuna sızmak mümkün olmayacaktır.

Ayrıca, soruşturmanın gözünden bakıldığında, bu yasadışı faaliyetlere suç isnat eden, gizli faaliyetlerin yürütülmesine izin veren ve elde edilen kanıtların mahkemede kabul edilebilir olmasını sağlayan ilgili mevzuatın yürürlükte olması önem taşımaktadır. Bu soruşturma; klasik soruşturma teknikleri ile internet tekniklerinin bir karışımıdır.

Bilinen bir yeraltı forumunun sahipleri veya işletimcilerinin ulusal bir yargı yetkisi alanı içerisinde bulunduğu ya da yeraltı forumunun barındırma servisini ulusal yargı yetkisi alanı içerisinde aldığı durumlarda, ulusal mevzuattaki ilgili esasa ilişkin hükümler bu türden davalarda cezai kovuşturmanın temeli olarak kullanılabilir. İlgili hükümler davanın

¹⁷Karanlık ağ piyasaları hakkında bilgi edinmek için bkz.: <https://www.deepdotweb.com/>

özelliklerine bağlı olacaktır ancak örneğin Budapeşte Sözleşmesi 6. maddesinin eşdeğeri olabilmektedir.

ÜZERİNE DÜŞÜNÜLECEK SORULAR

1. Şüpheli bir banka hesabının izlenmesine izin verilmeden önce hangi koşulların ortaya çıkması gerekmektedir?
2. Banka hesabının gizliliği ihlal edilmiş, potansiyel olarak masum bir üçüncü tarafın çıkarlarını korumak için nasıl bir dengenin izlenmesi gerekmektedir?
3. Bir şüpheliyi şifrelenmiş bir cihazın veya dosyanın şifresini çözmeye zorlamak için ulusal mevzuatınızda ne türden hükümler bulunmaktadır?
4. Ulusal bir internet hizmeti sağlayıcısını yasadışı içeriği engellemeye veya filtrelemeye zorlamak için ulusal mevzuatınızda ne türden önlemler bulunmaktadır?

2.2 Fail Kimliğinin Saptanması

Temel eğitimden hatırlayacağınız gibi internet üzerindeki bir şüphelinin saptanmasında kullanılan temel özellik onun İP adresidir.

Bu bölümün amacı; belirli bir İP adresi ile bir bireyi ilişkilendirmeye çalışırken ortaya çıkabilecek bazı pratik güçlükleri daha detaylı bir biçimde anlatmaktır. Bir başka ifadeyle, bazı internet suç faaliyetlerini belirli bir İP adresi ile ilişkilendirebildiğiniz ve söz konusu İP adresinin kontrolünü suç faaliyetinin gerçekleştiği anda elinde tutan gerçek dünya kişisini saptamaya çalıştığınız durumları ele alacağız.

Tersinden de elbette gerçek dünyadan bir şüpheliniz olabilir ve bu birey tarafından internette kullanılmakta olan İP adresini saptamaya çalışıyor olabilirsiniz. Pek çok bakımdan bu durumla baş etmesi daha kolay olacak ve geleneksel soruşturma teknikleri (özel soruşturma önlemleri gibi) kullanılabilecektir.

2.2.1 Ağ Adresi Çevirisi (NAT)

İnternet üzerinde iletişim kurmak için bir kaynak ve hedef İP adresi gerekmektedir. Geçmişte (NAT gündeme girmeden önce), her bir bilgisayarın kendisine atanmış benzersiz bir İP adresi olması gerekiyordu. Buradaki sorun şu ki İP adresleri verimsiz şekilde tahsis edilmekte ve bu nedenle tükenmekte. İP adreslerindeki darlığa getirilen uzun vadeli çözüm bir İP versiyonunun, İP versiyon 6'nın uygulamaya konmasıdır. Bu versiyonda çok daha fazla erişilebilir İP adresi bulunmaktadır. Bu arada, İP versiyon 4'ün ömrünü uzatmak için bazı teknikler kullanılmaktadır ve bu tekniklerden birisi de NAT'tır.

Ayrılmış bazı İP adresi aralıkları bulunmaktadır, yani bunların internette kullanılmayacağı varsayılmaktadır. Bunun yerine, iç ofis aralıkları türü özel ağlarda kullanılmaları amaçlanmaktadır. Ayrılmış aralıklar şunlardır:

1. 10.0.0.0 – 10.255.255.255

- a. Bir başka ifadeyle, "10." ile başlayan tüm İP adresleri.
2. 192.168.0.0 – 192.168.255.255
 - a. Bir başka ifadeyle, "192.168." ile başlayan tüm İP adresleri.
3. 172.16.0.0 – 172.31.255.255
 - a. Bir başka ifadeyle, "172." ile başlayan ve "16" ile "31" arasındaki bir sayıyla devam eden tüm İP adresleri.
 - b. Ayrılmış bu aralık diğer ikisine göre daha az sıklıkla kullanılmaktadır.

En yaygın NAT uygulaması bu aralıklardan birisinden gelen İP adreslerini tüm ofis bilgisayarlarına tahsis eden kuruluşları içermektedir. Ardından, ağlarındaki bilgisayarlardan birisi internet üzerindeki bir İP adresi ile iletişim kurmak istediğinde, yönlendiricileri iç İP adresinin yerine, bir dizi gerçek, internet İP adresinden birisini geçirmektedir ve gerçek İP adresleri dizisi dar bir aralık oluşturmaktadır. Çoğu örnekte, bu sürecin çıktısı ofis ağındaki tüm bilgisayarlardan gelen İP verilerinin internetin geri kalanına tek bir İP adresinden geliyor gibi görünmesidir.

Evlerdeki geniş bantlı internet kurulumlarında da NAT kullanımı son derece yaygındır, aslında sanal olarak her yerdedir. Bu; bir ev kullanıcısının evdeki ağı üzerinde birden fazla cihaz kullanabileceği fakat İnternet Servis Sağlayıcısının bağlantısına tek bir İP adresi tahsis etmesi gerektiği anlamına gelmektedir.

NAT'ın nasıl işlediğine dair pek çok başarılı teknik betimleme internette bulunmaktadır^{18, 19, 20}. İlgili okur eğer gerekli ise daha fazla bilgi edinmek için bu kaynakları gözden geçirebilir.

NAT kullanımının internet soruşturmaları açısından taşıdığı sonuçlar üzerinde durmak da değerlidir. Belirli bir suç faaliyeti sırasında kullanımda olan ortak İP adresini saptamak mümkün olabilmektedir ancak eğer NAT kullanılıyorsa, bu İP adresi pek çok bağımsız kullanıcının çevrimiçi faaliyetini temsil edebilmektedir. Dolayısıyla çevrimiçi faaliyet ile NAT yönlendiricisi gerisinde ayrılmış bir İP adresini kullanan bireysel kullanıcı bilgisayarı arasındaki bağlantıyı kurmak için ek bir soruşturma adımı gerekmektedir.

NAT kullanan bir kuruluşun, soruşturma konusu olan belirli bir akış parçasını üretmekten sorumlu iç İP adresini belirlemede kullanılan iç ve dış akış günlük kayıtlarına sahip olması uzak bir olasılık olarak mevcuttur. Ancak, çok muhtemel değildir. Ayrıca, İSS tarafından sağlanan standart ekipman ve hizmetleri kullanan küçük ofisler ve ev kullanıcıları türü örneklerde, bu tip kayıtlara erişilemez.

Dolayısıyla soruşturma şüpheli İP adresi ile belirli bir bilgisayarı bağlantılandırmak için alternatif bir mekanizma kullanılmalıdır. İç İP adresinin saptanabilmesini sağlayan belirli akış özellikleri olabilir. Örneğin, belirli uygulamalar akış içerisinde akışı oluşturan bilgisayarın iç İP adresini içermektedir. Alternatif olarak, İP adresi dışında, kullanılabilecek farklı ayırt edici özellikler olabilir. Bunlar kullanıcı adlarını, e-posta adreslerini, kaynak cihazla ilgili teknik bilgileri vs. içerecektir. Bir uzmanın yapacağı detaylı analizler sayesinde bu şekilde akışın kaynağını saptamak mümkün olabilmektedir.

Eğer suç faaliyeti gerçek zamanda vuku buluyorsa, dışarı yöndeki akışta araya girmek ve bu yolla iç bilgisayarı saptamak için özel soruşturma önlemleri uygulanabilir. Bu türden durumlarda bir izleme istasyonu kurmak üzere ağları üzerindeki uygun yeri saptamak için

¹⁸<http://computer.howstuffworks.com/nat.htm>

¹⁹<http://www.faqs.org/rfcs/rfc1631.html>

²⁰<https://www.youtube.com/watch?v=QBqPzHEDzvo>

kuruluşun işbirliği gerekli olabilir. Bu da tipik olarak bilgi teknolojisi/sistem yönetimi çalışanlarının işbirliğini içerecektir ve önceden şüphelinin bilgi teknolojisi/sistem yönetimi çalışanları arasından olmadığına emin olmanın herhangi bir yolu bulunmadığını akılda tutmak gerekir ki eğer öyle ise şüpheli soruşturmanın farkına varacaktır.

Özetle NAT, belirli bir İP adresi ile bir gerçek dünya kullanıcısının faaliyetini ilişkilendirmek konusunda güçlük yaratmaktadır. Tipik olarak, soruşturmanın tamamlanması ve şüphelinin saptanması için çevrimiçi faaliyet analizinden elde edilen (İP adresi dışındaki) ek bilgilere veya alternatif olarak ek soruşturma önlemlerine ihtiyaç duyulmaktadır.

2.2.2 Taşıyıcı Ölçeğinde Ağ Adresi Çevirisi (CGN)

Taşıyıcı ölçeğinde ağ adresi çevirisi ya da CGN kullanımı da ek güçlükler yaratmaktadır. CGN bir İSS'nin çok sayıda abone İP adresini az sayıda gerçek internet İP adresine dönüştürmek için NAT kullanabildiği bir tekniktir.

Bu örneklerde CGN şu anlama gelmektedir: akış küçük bir ofisten veya evden İSS ağına hareket ederken gerçekleşebilecek NAT bir yana, akış internete iletilmeden önce İSS'nin ağı içerisinde ikinci bir NAT gerçekleşebilir²¹, ²².

CGN bir önceki bölümde anlatılan "basit" NAT'tan farklıdır çünkü yalnızca özel (iç) İP adresi bir kamusal (dış) İP adresi ile değiştirilmekle kalmaz, ama aynı zamanda özel (iç) Aktarma Kontrol Protokolü/İP bağlantı noktası numarası bir kamusal (dış) bağlantı noktası numarası ile değiştirilir. Özünde CGN; bir iç adres alanından gelen Aktarma Kontrol Protokolü veya Kullanıcı Veri İletisi Protokolü oturumlarını bir dış adres alanına eşlemektedir. Bu teknik; "basit" NAT ile alakalı bazı ölçeklendirme meselelerinin üstesinden gelinmesine olanak tanımakta, ancak soruşturmanın bakış açısından bakıldığında bir sorun yaratmaktadır. Örneklerin büyük çoğunluğunda kuruluşlar bağlantı aldıkları İP adresini sistem günlüğüne kaydedecek fakat gelen bağlantı noktası numarasının sıralı kaydını tutmayacaktır. CGN potansiyel olarak binlerce kullanıcının aynı kamusal İP adresini kullanıyor olmasına olanak tanıdığı ölçüde, tek başına İP adresi faaliyetin belirli bir kullanıcı ile bağlantılandırılması için yeterli olmayacaktır.

Bu nedenle, bağlantı noktası numarasının erişilebilir olmadığı varsayıldığında, şüphelinin saptanması için (İP adresinden başka) çevrimiçi faaliyet analizinden gelen diğer ek bilgilere gerek olacaktır.

Europol, 2016 Organize İnternet Suçları Tehdidi Değerlendirmesi kapsamında, CGN nedeniyle ortaya çıkan soruşturma güçlükleri ile baş etmeye yönelik pek çok tavsiyede bulunmaktadır.²³ Söz konusu tavsiyeler şunları içermektedir:

- Bireysel son kullanıcıda CGN kullanan bir ağdaki İP adresinin izini bulabilmek için, kolluk kuvvetlerinin hukuki süreç üzerinden hizmet sağlayıcılarından ek bilgi talep etmesi gerekmektedir:
- Kaynak ve hedef İP adresi
- Kaynak bağlantı noktası numarası
- Tam bağlantı saati (saniyesi).

²¹Arka plan bilgileri için ek bağlantılara ulaşmak üzere bkz.: https://en.wikipedia.org/wiki/Carrier-grade_NAT.

²²<http://www.networkworld.com/article/2237054/cisco-subnet/understanding-carrier-grade-nat.html>

²³Organize İnternet Suçları Tehdidi Değerlendirmesi (IOCTA), Europol, 2016. Ulaşmak için bkz.: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016> ve 2017 için bkz.: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>

- Ancak Avrupa'da uyumlulaştırılmış veri saklama standardı gereklilikleri olmaması; içerik hizmeti, internet hizmeti ve veri barındırma hizmeti sağlayıcılarının bu türden bilgileri saklamak bakımından herhangi bir yasal yükümlülüğe tabi olmadıkları anlamına gelmektedir ki bunun da anlamı kolluk kuruluşundan gelen daha ayrıntılı bir talebin dahi, sağlayıcıdan kullanılabilir bilgi çıkarmayacağıdır.
- Son kullanıcıları saptamak için kolluk kuvvetlerinin ihtiyaç duydukları gerekli ek verileri (kaynak bağlantı noktası) içerik hizmeti sağlayıcılarının sistematik olarak saklamasını temin edecek düzenleyici/yasal değişiklikler gerekmektedir.
- Alternatif olarak, elektronik hizmet sağlayıcıları ile kolluk kuvvetleri arasında kurulacak işbirliği üzerinden pratik çözümler geliştirilebilmektedir. Avrupa'daki bazı elektronik sağlayıcılar, ilgili bilgileri saklamaktadır (kaynak bağlantı noktası). Avrupa çapındaki bir portal, CGN nedeniyle bir soruşturmada hız kesilmesi durumunda başvurmak üzere söz konusu sağlayıcıların güncel bir listesini ve bir iletişim bilgileri listesini kalıcılaştırabilir.

2.2.3 İP Numarasını Gizleyen (Anonimleştiren) Yazılımların Kullanılması

İP numarasını gizleyen yazılım internet üzerindeki faaliyeti izlenemez hale getirmeyi deneyen bir araçtır. Bir bilgisayar ile internetin geri kalanı arasındaki bir aracı gibi hareket etmekte ve kullanıcının kimlik bilgilerini saklarken kullanıcı adına internete erişmektedir.

İP numarasını gizleyen yazılımlar iki geniş kategori altında toplanabilmektedir;

- **Protokole özgü İP numarasını gizleyen yazılımlar:** Bunlar sadece belirli bir protokol ile çalışmaktadır. İmzasız e-posta göndericisi veya İP numarasını gizleyen ağ vekili örnek olarak gösterilebilir.
- **Protokolden bağımsız İP numarasını gizleyen yazılımlar:** Bunlar tüm kullanıcı akışının iletileceği bir İP tüneli yaratarak çalışmaktadır. Alan kullanıcının gözünden bakıldığında, İP akışı orijinal göndericiden başka birisinden geliyor gibi görünecektir. Bir örnek Tor (önceden "Soğan Yönlendirici" idi) olabilir.

Aşağıdaki vaka çalışmalarında bazı örnekler tartışılmaktadır.

İP numarasını gizleyen bir yazılımın kullanıldığı ve servis sağlayıcısının soruşturmaya destek sunmak istemediği veya sunmadığı durumlarda, ilerleme kaydetmek için alternatif (teknik olmayan) soruşturma önlemleri gerekli hale gelebilir.

VAKA ÇALIŞMASI: İMZASIZ E-POSTA GÖNDERİCİSİ

İmzasız e-posta göndericisinin amacı; mesajları almak, kimlik tanımlama bilgilerini ortadan kaldırarak bunları alıcının bunların nereden kaynaklandığını söyleyemeyeceği bir biçimde amaçlanan alıcıya nakletmektir.

Bu birden fazla yolla becerilebilmektedir:

- **Takma isimli e-posta göndericileri:** göndericinin e-posta adresini alır, göndericiye bir takma isim verir ve mesajı amaçlanan alıcıya gönderir. Alıcı takma isme e-posta göndererek cevap verebilecektir, bu cevabı e-posta göndericisi tekrar orijinal göndericiye iletacaktır.

- **Siberpunk (Cypherpunk) e-posta göndericileri (nam-ı diğer Tip I):** Mesajı alıcıya gönderici adresini ayırarak gönderirler. Alıcı bu tip bir e-posta göndericisinden gelen e-postaları yanıtlamaz. Genellikle mesajın göndericisi mesaj göndericisine mesajı şifrelenmiş biçimde iletacaktır. E-posta göndericisi mesajın şifresini çözecek ve mesajı alıcıya gönderecektir. Bu tip e-posta göndericileri işlemlerin sıralı kayıtlarını tutmamaktadır.
- **Mixmaster e-posta göndericileri (nam-ı diğer Tip II):** Gönderici bir e-posta oluşturur ve onu e-posta göndericisine gönderir. Mesaj; e-posta göndericilerinin denkler arası ağı üzerinden sonunda alıcıya ulaşana kadar birden fazla defa iletilir. Alıcı e-posta gövdesinde bir yanıt adresi verilmediği sürece e-postaya yanıt veremez. Bir mixmaster e-posta göndericisi kullanmak için kullanıcının bilgisayarına özel yazılım yüklenmesi gerekmektedir.
- **Mixminion e-posta göndericileri (nam-ı diğer Tip III):** Bunlar mixmaster e-posta göndericilerine benzemektedir ancak bazı teknik meseleler ele alınmıştır. Özel olarak, alıcının, göndericinin kim olduğunu bilmeksizin e-posta göndericileri ağı üzerinden yanıt vermesi mümkündür.

Çok sayıda e-posta göndericisini içeren bir zincir oluşturmak ve bu yolla e-posta göndericilerinin dahi mesajı kimin gönderdiğini bilmemesi mümkündür. Kullanıcı bilgisayarına kurulan standart veya özelleştirilmiş bir e-posta uygulaması yerine, bir e-posta göndericisine bağlanan internet tabanlı arayüz kullanılması da mümkündür.

VAKA ÇALIŞMASI: ANONİMLEŞTİREN AĞ VEKİLİ

Anonimleştiren bir vekil sunucu bir kullanıcının internet göz atma faaliyetini anonimleştirmeye çalışmaktadır. Tipik olarak anonimleştiren vekil, kullanıcılardan talepleri kabul edip bu talepleri iletacaktır. Talebi alan ağ sunucusunun gözünden bakıldığında, talep anonimleştiren vekilden geliyor gibi görünür. Anonimleştiren vekil, dışa giden talepleri belirli kaynak IP adresleri ile ilişkilendirecek kayıtlara sahip değilse, IP verilerinin analizinden bunu gerçekleştirmek mümkün olmayacaktır.

Hemen hemen tüm standart tarayıcılarda bir ağ sunucusunun kullanılması desteklenmektedir, zira kullanıcıların bir vekil yapılandırmayı istemekte pek çok meşru nedeni vardır²⁴. Bu hizmetlerin kullanımı tipik olarak standart tarayıcı yazılımında az sayıda seçeneğin yapılandırılmasından çok daha fazlasını gerektirmemektedir.

Ancak, internet akışının içeriği hala bir şüphelinin saptanmasına yardımcı olabilecek detaylar içerebilir. Örneğin, bir şüpheli bir anonimleştiren vekil aracılığıyla bir internet sitesine giriş yapacak olsa, giriş yaptıkları IP adresi mevcut olmayabilir, ancak internet akışının analizi, kullanılan kullanıcı adı ve/veya şifreyi ortaya çıkarabilir.

²⁴Örneğin, bir kuruluş, çalışanların iş saatlerinde belirli internet sitelerini görüntülemesini engellemek isteyebilir. Bu gibi durumlarda, çalışanların bilgisayarlarına bir vekil yapılandırılabilir ve internete doğrudan ağ erişimi bu sayede bir güvenlik duvarı tarafından engellenir. Dolayısıyla tüm ağ talepleri vekilden geçmelidir ve kurumsal olarak tanımlanmış bir politika göre talepleri bloke etmek veya taleplere izin vermek bu durumda vekile bağlı olacaktır.

VAKA ÇALIŞMASI: TOR (önceden “Soğan Yönlendirici” idi)

Tor, internet akışını gönüllülerin sahip olduğu, ücretsiz olarak çalıştırılan ve birkaç bin ileti anahtarlamasından oluşan bir bilgisayar ağı üzerinden yönlendiren bir yazılım aracıdır. Bunun amacı, internet faaliyetinin orijinal kullanıcıya dek geri izlenmesini zorlaştırmaktır.

Yönlendirme, çoklu şifreleme katmanları ve daha sonra çoklu, rastgele seçilmiş ileti anahtarlama yoluyla akışın iletilmesiyle gerçekleştirilir. Her ileti anahtarlama, sadece bir sonraki anahtarlama katmanını gösteren ve kalan şifrelenmiş veriyi ona aktaran bir şifreleme katmanı şifresini çözer. Son ileti anahtarlama, en içteki şifrelenmiş verileri çözer ve bu verileri kaynak İP adresini göstermeksizin veya bilmeksizin hedeflendiği varış noktasına gönderir. Dolayısıyla iletişimin yönlendirilmesi, Tor ağındaki her sıçramada kısmen saklanır, yani iletişim halindeki eş düzeylerin, iletişimin kaynağına ve hedefine dayanan veya onu saptayan bir biçimde izlenebildiği tek bir nokta yoktur.

Tor ağı kullanıcısı, bilgisayarına, giden ağ akışının bir bölümü veya tamamında araya girecek ve bu akışı doğrudan hedeflenen varış noktasına iletmek yerine Tor ağına iletecek özel bir yazılım yükler. Akış, Tor ağı içine girince, (son şifre çözmenin gerçekleştiği ve orijinal akışın gösterildiği) ağıdaki son yönlendiriciye ulaşıncaya kadar yönlendiriciden yönlendiriciye gönderilir. Bu yönlendirici çıkış düğümü olarak bilinir. Varış noktasının gözünden bakıldığında, akış çıkış düğümünden kaynaklanıyor gibi görünür.

Yukarıdaki açıklamadan, Tor ağının sadece kullanıcı tarafından başlatılan iletişim anonimleştirmesine izin verdiği düşünülebilir. Bununla birlikte, Tor, sunucunun İP adresi bu sunucunun kullanıcıları tarafından görülemeyecek bir biçimde Tor ağı üzerinden sunucuların çalışmasını da destekler. Bunu başarmak için sunuculara soğan adresleri olarak bilinen özel adresler verilir ve bunlara sunucunun yerini göstermeyecek bir şekilde Tor ağı üzerinden erişilebilir²⁵. Gizli bir hizmet varlığını duyurur ve daha sonra Tor ağı gizli hizmetler ile kullanıcılar arasındaki bağlantılara izin verecek şekilde merkezi olmayan bir biçimde “randevu noktaları” kurar. Burada gizli hizmetlerle kullanıcılar bir diğerinin kimliğini bilmez.

Tor ağı kullanan bir şüphelinin İP adresinin doğrudan saptanması neredeyse imkânsız olsa da, soruşturmayı ilerletebilecek diğer bilgileri saptamaya yönelik uzmanlaşmış teknikler bulunmaktadır. Örneğin, sunucu yanlış yapılandırmasının gizli hizmetin gerçek kaynağı hakkındaki bilgileri açığa çıkarması mümkündür. Pek çok yaygın ağ sunucusu tarafından üretilen hata sayfaları (yani, istekleri bir hataya neden olduğunda bir kullanıcıya verilen hata mesajı), sunucunun İP adresini içerir; bir diğer deyişle, sunucu üzerinde bir hata durumu oluşturarak İP adresi ortaya çıkarılması mümkün olabilmektedir.

²⁵Gizli hizmetlerin işleyişi hakkında daha fazla detay için bkz.: <https://www.torproject.org/docs/hidden-services.html>

2.2.4 Çok Sayıda Bilgisayarın bir İP'ye Saldırması / Kötü Amaçlı Yazılımlar / Bir Bilgisayarın Uzaktan Kumanda Edilmesi

Bir kişinin bilgisayarına kötü amaçlı yazılım bulaştığında, bilgisayara, şüpheli bir şahsın bilgisayarı kontrol edip onu suç oluşturan faaliyetlerde bulunmak için kullanabilmesini sağlayan yazılım yüklenmiş olması ihtimali vardır. Diğer ihtimaller arasında, şüpheli gizliliği ihlal edilmiş bilgisayara bir vekil yerleştirebilir ve bu vekil üzerinden tüm akışlarını gerçekleştirebilir.

Bu tür durumlarda, suç faaliyeti ile alakalı internet akışı masum tarafın İP adresinden geliyormuş gibi görünecektir. Ancak, akışın gerçek kaynağının saptanmasına izin verecek teknik önlemler alınması mümkündür. Örneğin, gizliliği ihlal edilmiş bilgisayara gelen ve bilgisayardan giden İP akışının izlenmesi yoluyla, bilgisayarı kontrol eden şüphelinin İP adresinin saptanması mümkün olabilmektedir. Bu, en fazla, bir suçlunun az sayıda bilgisayarın gizliliğini ihlal edip bunlarla bireysel olarak iletişim kurduğu durumlarda olasıdır.

Ancak, suçluların gizliliği ihlal edilmiş bilgisayar ağlarını işletmek için kullandıkları komuta ve kontrol altyapısının karmaşıklığı (bunlar kimi zaman büyük zombi bilgisayar ağı olarak bilinirler) hafife alınmamalıdır. Büyük zombi bilgisayar ağlarının işletmecileri tarafından faaliyetlerini gizlemek ve kontrol akışlarının güvenlik duvarlarından geçmesini sağlamak üzere pek çok teknik uygulanmaktadır^{26, 27, 28}.

Kişinin bilgisayarının analizi, bilgisayarın üçüncü bir tarafça uzaktan kontrol edilmiş olabileceği iddiasını destekler şekilde kötü amaçlı yazılımları ortaya çıkarabilmektedir. Ancak öte yandan, bir şüphelinin, bilgisayar üzerinden veya bilgisayar ile gerçekleştirilen eylemlerden sorumlu olmadığına yönelik bir savunmaya yaslanmak amacıyla bilgisayarına isteyerek kötü amaçlı yazılım bulaştırması olasılık dışı değildir. Bu nedenle, "şüpheliyi klavyeye oturtma" güclüğü, hangi bireyin hangi eylemleri gerçekleştirdiğinin ya da eşdeğer bir biçimde belirli bir bireyin suç oluşturan eylemleri gerçekleştirmiş olması olasılığının bulunmadığının saptanması için, izleme türünden teknik olmayan başka önlemlerin alınmasını gerektirebilmektedir.

Soruşturma görevlileri, kullanıcıyı bulaşan kötü amaçlı yazılımlar hakkında uyarma yolu ve kötü amaçlı yazılımları kaldırmak için kullanılacak uygun araçlar konusunda da güçlüklerle karşılaşmaktadır. Kullanıcıları kötü amaçlı yazılım bulaşmış bilgisayarları konusunda uyarma anı önem taşımaktadır ve bu konuya soruşturmanın durumuna bakarak karar verilmelidir. Kötü amaçlı yazılımların bulaşmış olduğu makinelerden bunların kaldırılması, usulüne uygun rıza/yetkilendirme olmaksızın gerçekleştirilen yasadışı erişimi ya da iletişimde araya girilmesini engelleyecek şekilde yapılmalıdır.

2.2.5 Açık, Kamusal ya da Çalıntı Kablosuz Bağlantı Kullanılması

Açık kablosuz ağ bağlantıları özel olarak herkesin onlara bağlanabilmesi ve interneti kullanabilmesi için kurulmaktadır. Açık kablosuz ağ bağlantıları, internete bağlanabilirliğin suç oluşturacak şekilde kullanılması riski oluşturmaktadır; öyle ki bu bağlantıları kullanan suç faaliyetlerini açık kablosuz ağ kaynağından başka herhangi bir kişiyle bağlantılandırmak mümkün olmayabilir. Tümü olmasa da bazı açık kablosuz ağ bağlantıları kayıt talep etmekte ve/veya günlük kaydı tutmaktadır.

²⁶https://en.wikipedia.org/wiki/Fast_flux

²⁷https://en.wikipedia.org/wiki/Domain_generation_algorithm

²⁸<http://www.pcworld.idg.com.au/article/417011/malware-increasingly-uses-dns-command-control-channel-avoid-detection-experts-say/>

Bir saldırganın kapalı kablosuz bağlantı ağının kablosuz bağlantı şifresini tahmin etmesinin veya kırmasının mümkün olduğu hallerde benzer bir sorun ortaya çıkmaktadır. İzinsiz girilen kablosuz bağlantı noktaları ve/veya çalıntı kablosuz bağlantı erişimi kullanımından doğan ve sıklıkla atıfta bulunulan bir senaryo, bir saldırganın bir ofis binası dışına arabasını park etmesi ve ofisin kablosuz bağlantılarını suç faaliyeti gerçekleştirmek üzere kullanmasıdır. Bu tür durumlarda, kimlik tespitine olanak tanıyan, kablosuz bağlantı ağına bağlanma kayıtlarının mevcut olması pek olası değildir (özellikle küçük işletmeler düşünüldüğünde), dolayısıyla şüphelinin yerini tespit edecek şekilde soruşturmanın sürdürülmesi mümkün olmayacaktır. Bir şüphelinin birden fazla sefer aynı yeri kullanması olasıdır, bu durumda mekânın izlenmesi şüphelinin saptanmasını sağlayabilir.

İnternet erişiminin görece olarak anonim bir biçimde sunulduğu, kütüphaneler, üniversiteler ve internet kafeler gibi pek çok mekân olduğundan, yukarıda anlatılanla bağlantılı bir sorun ortaya çıkmaktadır.

Bu sorunun tanımlayıcı özelliği, bir şüphelinin internete bağlanabilirliği ve bazı durumlarda üçüncü bir tarafa ait bilgisayarları kullanarak internete sanal olarak anonim erişim sağlayabilmesidir.

Bir önceki bölümün sonunda ortaya atılan sava benzer bir biçimde, kişinin ağının incelenmesi açık kablosuz ağın varlığını ortaya koyabilir, bu da kablosuz bağlantının üçüncü bir tarafça kullanılmış olabileceği iddiasını destekler. Ancak, bir şüphelinin kablosuz bağlantı üzerinden gerçekleştirilen eylemlerden sorumlu olmadığına ilişkin bir savunmaya yaslanmak üzere kablosuz bağlantısını kasten açık bırakması da olasılık dışı değildir. Bir kez daha, hangi bireylerin hangi eylemleri gerçekleştirdiğinin ya da eşdeğer bir biçimde belirli bir bireyin suç oluşturan eylemleri gerçekleştirmiş olması olasılığının bulunmadığının saptanması için izleme türünden teknik olmayan başka önlemlerin alınması gerekebilmektedir.

Suç faaliyetlerine farklı bireylerin dahilini belirlemek üzere kullanılabilecek bir başka teknik ise internet iletişiminde araya girilmesidir.

2.2.6 Bir İP Adresi Sahibinin Kimliğinin Saptanması

WHOIS; ad, soyadı ve iletişim bilgileri de dâhil olmak üzere, bir alan adının sahibi hakkında bilgi sağlayan ücretsiz bir hizmettir.

Dünya genelindeki alan adı yöneticisi İnternet Tahsisli Sayılar ve İsimler Kurumu'na (ICANN)²⁹ göre, "WHOIS hizmeti, kayıtlı alan adı hizmet kaydı yapılmış kişilere ilişkin iletişim bilgileri ve teknik bilgiler içeren, kamuya açık bir rehberdir. Bir internet sitesi alan adı arkasında kimin olduğunu bilmek isteyen herkes WHOIS üzerinden bu bilgiyi talep edebilmektedir.

Veriler; ICANN ile girdikleri anlaşmaların şartları çerçevesinde, kayıt görevlileri ve kayıt kuruluşları tarafından toplanmakta ve erişilebilir kılınmaktadır. WHOIS merkezi olarak yönetilen, tek bir veri tabanı değildir. Bunun yerine, kayıt verileri ayrı yerlerde tutulmakta ve çok sayıda kayıt kuruluşu ve kayıt görevlisi tarafından idare edilmektedir. ICANN ile sözleşmelerinde belirlenen asgari gerekliliklerle tutarlı bir biçimde WHOIS hizmetine yönelik olarak kendi kurallarını oluşturmaktadırlar".

WHOIS, belirli bir İP adresinin kime tahsis edildiğini bulmak için kullanılmaktadır. Sorun, WHOIS bilgileri veri tabanının her zaman doğru olmamasıdır. Kayıt görevlilerinin,

²⁹İnternet Tahsisli Sayılar ve İsimler Kurumu, internet kayıt kuruluşları ve kayıt görevlilerine yönelik olarak politikaları ve ilgili sözleşmeleri belirlemekle görevli uluslararası kurumdur.

bünyelerinde kayıtlı olan kişilere düzenli aralıklarla mesaj yollamaları gerekmektedir, ancak kayıt yapanın sağlamış olduğu verilerin doğruluğunu teyit etmek konusunda herhangi bir mesuliyetleri yoktur. Bu, özellikle belirli bir alan adına kimin sahip olduğunu saptamaya çalışırken sorun olmaktadır.

İP adresleri söz konusu olduğunda, başka bir sistem sorunu saptanmıştır ki bu İP adreslerinin alt-tahsisi konusudur³⁰. Sorun; bir dizi İP adresinin atanmış olduğu bir sağlayıcının bu İP adreslerinden bazılarını bir alt-sağlayıcıya atadığı, ancak İP adreslerini kimin kullandığına ilişkin olarak doğru veya güncel bilgilerin kaydını tutmadığı durumda ortaya çıkar. Özellikle sağlayıcı, alt tahsisi, WHOIS veri tabanı kaydına her zaman rapor etmeyebilir; bu da WHOIS veri tabanının söz konusu İP adresinin nihai denetleyicisi hakkında doğru bilgileri içermeyeceği anlamına gelir.

WHOIS verileri, abone bilgileri verileri bakımından, sınırsız erişime açık, internet üzerinde herkese açık olan özel bir biçim olarak görülebilir. Ancak, 25 Mayıs 2018 tarihinde AB Genel Veri Koruma Yönetmeliği'nin (GVKY) yürürlüğe girmesi ışığında, GVKY ile uyumu güvence altına almak üzere WHOIS'e erişim değişecektir³¹.

ÜZERİNE DÜŞÜNÜLECEK SORULAR

1. Bir İP adresinin izlenmesi emri, masum üçüncü tarafların haklarını etkilemeyecek bir biçimde yazılabilir mi?
2. Belirli bir İP adresi ile bağlantılı faaliyetin söz konusu İP adresinin sahibi tarafından mı gerçekleştirildiğini yoksa bilgisayara kötü amaçlı yazılım bulaştığı için uzaktan mı gerçekleştirildiğini belirlemek nasıl mümkün olabilir?
3. Gerçek dünyadan belirli bir şüphelinin kullanmakta olduğu İP adresinin saptanmasını sağlayabilecek bir emir çıkarmak için hangi koşulların oluşması gerekmektedir?
4. Bir suç faaliyetinde kullanılmış olan bir İP adresinin gerçek dünyadaki sahibinin saptanmasını sağlayabilecek bir emir çıkarmak için hangi koşulların oluşması gerekmektedir?

2.3 İSS'ler ile İlişkiler

2.3.1 Talep Edilen Verilerin Türü

Bir ceza soruşturması açısından, üç tür veriye ihtiyaç duyulabilmektedir:

- Abone bilgileri
- Akış verileri
- İçerik verileri.

Pek çok yargı yetkisi alanında, abone bilgilerine erişim şartları akış verilerine erişim şartlarından daha hafiftir ve en katı rejim içerik verilerine uygulanmaktadır. Talep edilen verilerin türü açık ki verilere erişim sağlamak için çok uluslu bir hizmet sağlayıcısına yapılması gereken talebin niteliğini etkileyecektir. Tümü olmasa da bazı çok uluslu hizmet sağlayıcıları, resmi yasal süreci beklerken, abone bilgilerini sağladıkları hızlandırılmış bir gönüllü işbirliği biçimini uygulamaktadır.

³⁰<https://blog.apnic.net/2016/11/28/sub-allocation-system-undermines-integrity-whois-accuracy/>

³¹ WHOIS'e erişim konusunda daha fazla okuma için bkz.: <https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance>

2.3.1.1 Abone bilgileri

Abone bilgileri; yerel soruşturmalarda ve ceza soruşturmalarında en sık aranan bilgilerdir ve bu bilgiler olmaksızın bir soruşturmanın ilerlemesi çoğu zaman mümkün olmamaktadır³². Abone bilgileri terimi, Budapeşte Sözleşmesi'nin 18.3 sayılı maddesinde şöyle tanımlanmaktadır:

"Bu maddede, "abone bilgileri" terimi, bir hizmet sağlayıcısı tarafından, akış ve içerik verileri dışında, hizmetlerinin aboneleri ile alakalı olarak tutulan bilgisayar verileri biçimindeki veya başka herhangi bir biçimdeki her türlü bilgiyi ifade etmektedir ve bu bilgilerle aşağıdakiler belirlenebilmektedir:

- a. Kullanılan iletişim hizmeti türü, ilaveten alınan teknik şartname ve hizmet dönemi;*
- b. Hizmet sözleşmesi veya düzenlemesi temelinde erişilebilir olan, abone kimliği, posta adresi ve coğrafi adres, telefon ve diğer iletişim numaraları, faturalandırma ve ödeme bilgileri;*
- c. Hizmet sözleşmesi veya düzenlemesi temelinde erişilebilir olan, iletişim ekipmanlarının kurulma yerine ilişkin diğer bilgiler."*

Abone bilgilerinin hizmet sağlayıcıları tarafından muhafaza edilmesi olasıdır; ancak söz konusu bilgiler fiilen bir başka yargı yetkisi alanındaki sunucularda depolanıyor olabilir. Dolayısıyla abone bilgileri açısından bir talebin kime yönlendirileceği her zaman açık olmayabilir.

2.3.1.2 Akış Verileri

Bir bilgisayarın işletim sistemi veya başka yazılım veya bilgisayarlar arası iletişim faaliyetlerini kaydeden günlük kaydı dosyaları siber suç davaları açısından hayati önemdedir ve internet kaynaklı suç gelirlerini içeren davalarda da aynı derecede önemli olabilmektedir. "Akış verileri" Budapeşte Sözleşmesi'nin 1.d sayılı maddesi kapsamında şöyle tanımlanmaktadır:

"Akış verileri bir bilgisayar sistemi yardımıyla bir iletişim ile ilişkilenen, iletişim zincirinde bir parça oluşturan bir bilgisayar sistemi tarafından üretilen, iletişimin kaynağını, varış noktasını, yönünü, saatini, tarihini, büyüklüğünü, kalıcılığını veya altta yatan hizmet türünü gösteren her türlü bilgisayar verisi anlamına gelmektedir."

2.3.1.3 İçerik Verileri

Son olarak içerik verilerine de ceza soruşturmalarında sıklıkla ihtiyaç duyulmaktadır. Budapeşte Sözleşmesi'nin Açıklayıcı Raporu'nun 209. paragrafına göre:

"İçerik verileri Sözleşme'de tanımlanmamaktadır fakat iletişimin içeriğine atıfta bulunmaktadır; yani iletişimin anlamı veya meali ya da iletişim tarafından aktarılan (akış verileri dışındaki) mesajı veya bilgileri ifade etmektedir."

Hâlihazırda bir bilgisayar sistemi üzerinde erişilebilir olan "depolanmış" içerik verileri ile henüz erişilebilir olmayan ve örneğin iletişimde araya girilmesi yoluyla "gelecekte ortaya çıkacak" içerik verileri arasında da bir ayrım yapılmalıdır. İletişimde araya girme bir mahkeme emrine binaen, polis tarafından ya da doğrudan uzmanlaşmış bir organ tarafından ya da hizmet sağlayıcısının yardımıyla gerçekleştirilebilmektedir. Kullanımı çoğu zaman ciddi suçlarla sınırlıdır.

³²12. Genel Oturum'da benimsenen, abone bilgilerinin elde edilmesi ile ilgili kurallar konulu Siber Suçlar Sözleşmesi Komitesi Raporu, 2-3 Aralık 2014.Ulaşmak için bkz.: <https://rm.coe.int/16802e7ad1>

2.3.2 Avrupa Birliği Adalet Mahkemesi Kararı ile Geçersiz İlan Edilen AB Veri Saklama Direktifi

Yukarıda tarif edildiği gibi, siber dünyada failerin saptanması pek çok defa özel internet hizmet sağlayıcılarının elindeki verilere erişime yaslanmaktadır. Bir şahsın (bir İP adresinin, e-posta veya Facebook hesabının abonesi) verileriyle bir İP adresinin bağlantısı, şüphelinin diğer olası şüphelilerle etkileşimi (akış verileri) ve hatta bu türden etkileşimlerin içeriği, failin, diğer şüphelilerin keşfedilmesinin ve bir suçun kanıtlarının güvence altına alınmasının esaslı bir kısmını oluşturmaktadır.

Tüm bunlar ancak eğer özel şirket gerekli verileri (abone verileri, akış verileri ve/veya içerik verileri) saklıyorsa mümkün olabilmektedir. Kolluk amaçlarıyla verilerin saklanması yönelik yasal yükümlülüğe Avrupa Birliği Adalet Mahkemesi nezdinde itiraz edilmiştir³³. Birlikte görülen C-93/12 ve C-594/12 davalarındaki (Digital Rights Ireland ile Seitlinger ve Diğerleri) kararında, 2006/24/EC³⁴ sayılı Verilerin Saklanması Direktifi geçersiz ilan edilmiştir. Ardından, karar, sağlayıcıların akış verilerini 6 ay ila 2 yıl arasında bir süre boyunca saklama yükümlülüğü taşıdığı bazı AB ülkelerinde ilgili ulusal mevzuatın iptaline yol açmıştır.

Sonuç; İSS'lerin, önceden ulusal mevzuatın talep ettiği süreler boyunca ve ciddi suçların soruşturulması amacıyla saklanan akış verilerini artık saklamak (muhafaza etmek) zorunda olmamasıdır, artık verileri yalnızca faturalandırma ve diğer ticari kullanımların gerektirdiği süreler boyunca saklamaktadırlar. Bu da pratikte 1-3 ay anlamına gelmektedir. AB henüz yeni bir yasal araç benimsememiştir ve pek çok devlet yasal kaygılar karşısında uygun yasal çözümleri tanımlamaya devam etmektedir. Öte yandan, ciddi suçlara karşı mücadele amacı göz önünde bulundurulduğunda, Mahkeme'nin herhangi bir farklılaştırma, sınırlandırma veya istisnaya başvurmaksızın, tüm bireylerin, tüm elektronik iletişim araçlarının ve tüm akış verilerinin, genelleştirilmiş bir biçimde kapsanmasından kaçınılması beklentisi özellikle güçtür.

Olası yaklaşımlardan birisi, sınırlı bir süre için hukuki talepte bulunulduktan sonra (akış) verileri(ni)n depolanması emrinin çıkarılmasına yönelik düzenlenme içerebilir.

Kanun tadili nedenlerinden birisi; direktifin, özel hayatın korunmasına ve kişisel verilerin korunmasına yönelik temel haklara ciddi bir biçimde müdahale ettiği için ölçülülük ilkesinin sınırlarını aştığına dönük mahkeme görüşüne dayandırıldığından, bu kararın, özellikle ulusal mevzuata ulusal anayasa mahkemelerinde itiraz edilmesi veya Avrupa İnsan Hakları Mahkemesi'ne İnsan Hakları Sözleşmesi'nin 8. maddesinin ihlal edilmesi nedeniyle bireysel şikâyetle bulunması halinde, AB üyesi olmayan devletlere de etkisi olabilecektir.

Bu nedenle, mahkeme kararının ana vurguları, ulusal yasa koyucuların ilgisini çekebilir. Mahkeme, direktifin özel yaşama saygı ve kişisel verilerin korunması konusundaki temel haklara özellikle ciddi bir şekilde müdahale ettiğini tespit etmiştir. Ayrıca, direktifin, ilgili kişilerde özel hayatlarının sürekli gözetleme konusu olduğu hissini yaratması olasıdır.

³³Birlikte görülen C - 293/12 ve C - 594/12 davalarında Avrupa Birliği Adalet Mahkemesi Hükümü. Digital Rights Ireland ile Seitlinger ve Diğerleri. Ulaşmak için bkz.: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

³⁴Kamusal olarak erişilebilir olan elektronik iletişim hizmetleri veya kamusal iletişim ağları sunumu ile bağlantılı olarak üretilen veya işlenen verilerin saklanması hakkında, 15 Mart 2006 tarihli ve 2006/24/EC sayılı Direktif ve değişiklikler, 2002/58/EC sayılı Direktif.(Geçersiz)

Mahkeme, direktifin, haberleşmenin içeriğini düzenlemediğini ve yetkili ulusal makamlara olası aktarım amacıyla verilerin saklanmasıyla gerçekten de genel çıkar hedefini, yani ciddi suçlarla mücadele ve sonuçta kamu güvenliği hedefini yerine getirdiğini belirtmiştir. Ancak, yasama organı, ölçülülük ilkesine uygunluğun dayattığı sınırlamaları aşmış olup yasa koyucunun takdirine yönelik incelemenin sıkı olması gerektiğine dikkat çekilmektedir.

Direktifin gerektirdiği şekilde verilerin saklanması, amaçladığı hedefe ulaşılması açısından uygun kabul edilebilse bile, direktifin özel yaşama saygı ve kişisel verilerin korunması konusundaki temel haklara geniş kapsamlı ve özellikle ciddi bir biçimde müdahale ediyor oluşu, ölçülülük ilkesine uygunluğun dayattığı sınırlamaların aşılmasına neden olmuştur, şöyle ki:

- Söz konusu müdahalenin kesinlikle gerekli olan şeyle sınırlı olmasını temin edecek şekilde yeterince sınırlandırılmış değildir,
- Genel bir şekilde, ciddi suçlara karşı mücadele amacı göz önünde bulundurularak herhangi bir farklılaştırma, sınırlandırma veya istisnaya başvurmaksızın tüm bireyleri, tüm elektronik iletişim araçlarını ve tüm akış verilerini kapsamaktadır,
- Yetkili ulusal makamların verilere erişebilmesinde nesnel bir ölçüt yoktur ve yalnızca, bu tür müdahaleleri haklı gösterecek kadar ciddi sayılabilecek suçlarla ilgili olarak önleme, tespit veya cezai kovuşturma amaçlarıyla kullanılabilecekleri belirtilmiştir. Basitçe "ciddi suçlar"a atıfta bulunmaktadır,
- Verilere erişim, bir mahkeme veya bağımsız bir idari organ tarafından önceden yapılmış incelemelere dayandırılmamaktadır,
- İlgili şahıslar temelinde veri kategorileri veya verilerin olası faydaları arasında herhangi bir ayırım yapmaksızın en az altı aylık bir saklama süresi dayatmaktadır,
- Süre en az altı ay ile en fazla 24 ay arasında bir süre için belirlenmektedir, ancak saklama süresinin kesin olarak gerekli olan şeyle sınırlandırılacak şekilde belirlenmesine ilişkin herhangi bir objektif kriter yoktur,
- Verilerin kötüye kullanıma riskine karşı etkin bir şekilde korunmasını temin edecek yeterli emniyet tedbirlerinden yoksundur,
- Veri saklama süresinin sonunda verilerin geri dönüşsüz şekilde yok edilmesini temin etmemektedir.

Kararın etkisine ilişkin olarak daha fazla okuma yapmak isterseniz, Franziska Boehm ve Mark D. Cole, 30 Temmuz 2014 tarihli, Avrupa Birliği Adalet Mahkemesi Kararı sonrası Verilerin Saklanması başlıklı makalelerinde, kimi ilgili noktaların altını çizmişlerdir³⁵. Mahkemenin beyanlarının tek başına Direktif örneğine atıfta bulunmadığını, aynı zamanda benzeri veri saklama önlemleri için genel ilkeler de tesis ettiğini vurgulamışlardır. Söz konusu ilkeler aşağıdaki hususları kapsamaktadır:

- Verilerin toplanması, saklanması ve aktarılması süreçlerinin her birisi 7 ve 8. maddelere yönelik ihlal oluşturmakta ve katı bir zorunluluk ve ölçülülük testi gerekmektedir.
- Mahkeme saklanan verilerin sınırsız şekilde veya hatta uzun süreler boyunca saklanmasına olduğu kadar şüpheli olmayan kişilerin umumi veri saklama süreçlerine tabi kılınmasına da açıkça karşı çıkmaktadır.

³⁵Avrupa Birliği Adalet Mahkemesi Kararı Sonrası Verilerin Saklanması, Prof. Dr. Franziska Boehm ve diğ., Munster/Lüksemburg, 30 Haziran 2014.Ulaşmak için bkz.: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

- Mahkeme, ilk başta farklı amaçlarla toplanan verilerin daha sonra kolluk amacıyla kullanılmasında hassas bir sorun görmektedir. Kamu güvenliğine yönelik bir tehdit ile bu türden amaçlarla saklanan veriler arasında bir bağlantı aramaktadır.
- Söz konusu bağlantı özel ve kamusal aktörler arasındaki ilişkiyi kayda değer biçimde etkilemektedir. Kolluk kuvvetlerine sadece belirli durumlarda başka amaçlarla toplanan verilere erişme izni verilmektedir.
- Mahkeme, bağımsız gözetim ve erişim kontrolü gibi etkili usul kurallarını açıkça talep etmektedir.
- Kolluk amacıyla verilerin toplanması ve kullanılması, kolluk kuruluşlarının veri tabanlarına verilerin dâhil edilmesinden kaynaklanan damgalama riskini beraberinde getirmektedir. Bu riskin kolluk kuruluşları ve Üye Devletler düzeyinde mevcut veya planlanan diğer veri saklama önlemlerini gözden geçirirken göz önünde bulundurulması ve hesaba katılması gerekmektedir.

Avrupa Birliği Adalet Mahkemesi'nin 29 Kasım 2016 tarihli kararının ortaya çıkardığı meselelerin ele alınabilmesi için, İngiltere 2016 tarihli Soruşturma Yetkileri Kanunu'nu kabul etmiştir. Diğer önemli tekniklerin yanı sıra, İSS'lere "bağlantı verilerini" 12 ay boyunca saklama yükümlülüğü getirmektedir. Bu, tüm göz atma verilerinin kaydedilmesine kıyasla daha düşük bir ihlal biçimidir ve Avrupa Birliği Adalet Mahkemesi'nin ölçsüz ihlal kaygılarını gidermek üzere tasarlanmıştır. Ayrıca, bir müzekkere yetkisiyle, şüphelinin göz atma vs. verilerinin yönlendirilmiş bir biçimde izlenmesine ve saklanmasına izin veren yeni yetkiler oluşturmaktadır.

2.3.3 Ulusal İSS'ler

İnternet Hizmet Sağlayıcılarının (İSS'lerin) sakladığı veriler failin ve suç ortaklarının, zaman ve mekân içinde aralarındaki bağlantının seyrinin saptanmasında ve iletişim içeriğindeki (e-posta içeriği, Facebook gibi sosyal platformlardaki paylaşımlar) kanıtlar açısından önem taşımaktadır.

İSS'lerin yükümlülükleri; (akış) verileri(ni)n saklanmasına ve ceza soruşturmalarının amaçları doğrultusunda bu verilere erişim ve bu verilerin kullanımı koşullarına ilişkin ulusal hükümler ile düzenlenmektedir. Veriler; abone verileri, akış verileri ve içerik verileri olarak kategorize edilebilmektedir.

Abone verilerinin akış verileri ve içerik verilerine kıyasla mahremiyet açısından daha az hassas olduğu düşünülmektedir. Siber suç ve elektronik kanıtlar ile ilişkili ulusal ve uluslararası ceza soruşturmalarında en fazla aranan bilgiler bunlardır. Bu bilgiler olmadan, bir soruşturmada ilerlemek genellikle mümkün olmamaktadır.

Abone verileri genellikle özel İSS'lerin elinde olmakta ve polis veya savcı emriyle elde edilebilmektedir. Ancak dinamik İP adresleri söz konusu olduğunda, bazı akış verileri işin içine girdiğinden pek çok devlet mahkeme emri istemektedir. Pek çok devlette mahkeme emri şunlar için talep edilmektedir: akış verilerine erişim (veri saklama konusu için önceki bölüme bakınız); muhafaza emri (emrin çıkarılmasından itibaren akış verilerinin depolanması); akış verilerinin izlenmesi; içerik verilerine erişim ve özel olarak da iletişimlerde araya girilmesi (sonucusu en müdahaleci önlem olarak görülmektedir ve bu nedenle belirli emniyet önlemlerine, şartlara ve ölçülülük ilkesine tabidir).

Yasal gerekliliklere ek olarak, İSS'ler ile kolluk kuvvetleri arasındaki veri aktarımına yönelik pratik ve teknik düzenlemeler de, özellikle verilerin hızla işlenmesine izin veren canlı izleme ve veri aktarımı söz konusu olduğunda, önem taşımaktadır.

Kolluk kuvvetleri ile İSS'ler arasındaki bir başka işbirliği alanı, ceza gerektiren suç veya ceza gerektiren içerik söz konusu olduğunda, internet sitelerinin engellenmesi ve kapatılması meselesidir. Bu bağlamda en fazla çocuk pornografisi malzemelerine atıfta bulunmaktadır, ancak nefret söylemi ve terör suçlarının işlenmesi veya fikri mülkiyet haklarının ihlali için halkın kışkırtılması gibi başka biçimler de söz konusu olabilmektedir. Genellikle bu türden bir önlem için mahkeme emri gerekecekse de, internet sayfasının sahibinin veya editörünün iç davranış kurallarının ihlali gerekçesiyle "gönüllü" şekilde önlem alması teşvik edilmektedir. Bu yaklaşım özellikle (pornografi malzeme örneğinde olduğu gibi), ilk bakışta haklı görülen ihlallerde en verimli yaklaşım olmaktadır; fakat internet üzerindeki yasadışı içeriğin filtrelenmesi, engellenmesi ve kaldırılması ile ilgili, 2016 tarihli Avrupa Konseyi Çalışması'nda ortaya konulduğu gibi, bu yaklaşım, ifade özgürlüğüne olası müdahaleler ile alakalı olarak bazı endişelere neden olabilmektedir³⁶.

ÜZERİNE DÜŞÜNÜLECEK SORULAR

1. "Abone bilgileri" terimi ile ne ifade edilmektedir?
2. "Akış verileri" terimi ile ne ifade edilmektedir?
3. "İçerik verileri" terimi ile ne ifade edilmektedir?
4. Verilerin muhafaza edilmesi ile ilgili Avrupa Birliği Adalet Mahkemesi kararının, suç faaliyetiyle ilişkilendirilen bir İP adresinden yola çıkarak gerçek dünyadan bir şüphelinin saptanması konusunda getirdiği sonuçlar nelerdir?

2.4 Çok Uluslu Hizmet Sağlayıcıları

İnternet kaynaklı suç gelirlerini içeren davalarda, pek çok siber suç ceza soruşturmasında olduğu gibi, çok önemli kanıtlar Facebook, Google, Microsoft, Twitter, Yahoo! vb. türünden özel sektör kuruluşlarının elinde olmaktadır. Yetkili makamlar ile bu çok uluslu hizmet sağlayıcıları arasındaki işbirliği, bu nedenle, elektronik kanıtların güvence altına alınması açısından son derece önemli olmaktadır. Elinizdeki el kitabı gibi bir kaynaktan, potansiyel okuyucunun ilişkiye girmesi gerekebilecek tüm farklı çok uluslu hizmet sağlayıcılarına dair bilgi vermek mümkün değildir; her bir hizmet sağlayıcısının, kolluk taleplerini ele alma sürecine ilişkin detaylar genellikle internet sitelerinde bulunabilmektedir. Dolayısıyla, çok uluslu hizmet sağlayıcılarının kolluk politikalarının kilit özellikleri kategorize edilmeye çalışılmıştır.

Burada amaç; gelecekte belirli bir hizmet sağlayıcısı ile nasıl ilişki kurulacağına dair düşünmeye yönelik bir çerçeve sağlamaktır. İkincil olarak, gelen kolluk taleplerini incelerken çok uluslu hizmet sağlayıcılarının hesaba katacağı faktörlerin, dolayısıyla başarılı bir çıktı olasılığını azamileştirmek için hizmet sağlayıcısına dönük bir talep oluştururken hesaba katılması gereken faktörlerin açıklığa kavuşturulmasına da yardımcı olacaktır.

Bulut Kanıtları Grubu (BKG); çok uluslu hizmet sağlayıcıları tarafından elde tutulan verilere kolluk kuvvetlerince erişim konusunda kapsamlı bir doküman hazırlamıştır³⁷. Bölüm **Error! Reference source not found.** kapsamında çok sayıda ilginç başlık daha derinlemesine ele alınacaktır. Bunlardan bazılarının altını çizmek gerekirse:

³⁶İnternet üzerindeki yasadışı içeriğin filtrelenmesi, engellenmesi ve kaldırılması ile ilgili, Avrupa Konseyi Çalışması, Haziran 2016. Ulaşmak için bkz.:

<https://www.coe.int/en/web/siber-suc/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>

³⁷ T-CY (2016)5, Buluttaki elektronik kanıtlara ceza yargılaması erişimi: Siber Suçlar Sözleşmesi Komitesi dikkatine sunulan tavsiyeler, Nihai Rapor, 16 Eylül 2016. Ulaşmak için

bkz.: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

- BKG, hukuki yardımlaşmanın, yerel ceza kovuşturmalarında kullanılacak, yabancı yargı yetkisi alanlarından gelen elektronik kanıtların elde edilmesinde başlıca araç olduğu sonucuna varmaktadır. İçerik verileri için bu özellikle doğrudur.
- Abone bilgilerine erişim daha düşük bir müdahale düzeyine denk düşmektedir ve hafifletilmelidir. Yurtiçi emirlere ilişkin 18. madde, bir devletin egemenlik alanında faaliyet gösteren çok uluslu İSS'lere yönelik olarak da kullanılmalıdır – abone bilgilerinin çıkarılması emirleri konulu, 10 numaralı taslak Kılavuz notu.
- Hukuki yardımlaşma taleplerindeki hızlı artış da hesaba katılarak, ABD'li İSS'lerin yabancı kolluk kuvvetleriyle gönüllü doğrudan işbirliği kabul edilmiştir.
- BKG bazı mevcut güçlükleri ele almak üzere, yani abone verilerine erişmek için ve belirli koşullar altında İSS'lere doğrudan talepte bulunulmasına izin verecek şekilde rejimin hafifletilmesi için ek protokol hazırlanmasının düşünüldüğünü önermiştir.

2.4.1 Yargı Yetkisi

Gerekli verilerin hangi yargı yetkisi alanında depolandığı ve/veya verilere hangi yasal rejimin uygulandığı, bir ceza yargılaması makamı için çoğu zaman belirgin değildir³⁸. Bir hizmet sağlayıcısının merkez ofisi bir yargı yetkisi alanındayken, ikinci bir yargı yetkisi alanının yasal rejimi geçerli olmakta ve veriler üçüncü bir yargı yetkisi alanında depolanmaktadır. Eğer verilerin yeri yargı yetkisi alanını belirliyorsa, hizmet sağlayıcısının verilerin yerini kolaylıkla bilememesi de mümkün olabilmektedir. Verilerin yeri biliniyor olsa bile, ceza yargılaması makamları tarafından gerçekleştirilecek kanuni erişim için hangi kuralların geçerli olduğu açık olmamaktadır. Yargı yetkisi alanını, hizmet sağlayıcısının veya alt kuruluşunun merkez ofisinin bulunduğu yerin ya da verilerin yerinin ya da şüphelinin söz konusu hizmete abone olduğu devletin hukukunun ya da şüphelinin yerinin veya yurttaşlığının belirleyebileceği iddia edilebilmektedir³⁹.

2.4.2 Genel Durum

Tüm örneklerde (aşağıda tartışılan fevkalade hal talepleri dışında), içerik verilerine erişim sağlamak için Hukuki Yardımlaşma sürecinin takip edilmesine gerek olacaktır.

Abone verileri söz konusu olduğunda, çok uluslu İSS'ler kabaca iki kategoriye ayrılabilir; Birleşik Devletler dışındaki yargı yetkisi alanlarından gelen hukuki taleplere yanıt verecek olanlar ve bir Birleşik Devletler mahkemesi tarafından kendilerine gönderilen Hukuki Yardımlaşma anlaşması talebini isteyecek olanlar.

2.4.3 Muhafaza Talepleri

Bazı hizmet sağlayıcıları muhafaza taleplerini kabul edecek ve bu sayede resmi yasal dokümanların alınmasını bekleyerek, belirli bir süre (genellikle 90 gün civarında) verileri muhafaza edecektir. Eğer 90 günden daha uzun süre muhafaza gerekirse, 90 günlük süre sona ermeden önce, hizmet sağlayıcısına bir uzatma mektubu gönderilmesi gerekmektedir.

³⁸Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu tarafından hazırlanan müzakere dokümanı, Buluttaki verilere ceza yargılaması erişimi: güçlükler, Mayıs 2015. Ulaşmak için bkz.:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>

³⁹T-CY (2016)5, Buluttaki elektronik kanıtlara ceza yargılaması erişimi: Siber Suçlar Sözleşmesi Komitesi dikkatine sunulan tavsiyeler, Nihai Rapor, 16 Eylül 2016. Ulaşmak için bkz.:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

2.4.4 Fevkalade Hal Talepleri

Hasar, ölüm ya da ciddi fiziksel yaralanma riskinin an meselesi olduğu durumlarda, hizmet sağlayıcısının söz konusu hasar, ölüm ya da ciddi fiziksel yaralanmayı önlemek için gerekli olabilecek bilgilere sahip olduğunun kanıtlanabildiği hallerde, çoğu çok uluslu hizmet sağlayıcısı bilgiye yönelik kolluk talepleriyle işbirliği yapacaktır. Bu bakımdan, bu eğitimde bir başka yerde⁴⁰ altı çizilen pratik bir güçlük şu ki pek çok ülkenin yürürlükte fevkalade hallerde yerli ceza yargılaması makamlarına verilerin ifşa edilmesine izin veren bir mevzuatı bulunmamaktadır. Hususi olarak ABD’de bu türden bir hüküm olduğunu belirtmek gerekir; söz konusu hüküm ABD temelli çok uluslu hizmet sağlayıcılarının fevkalade hal taleplerine yanıt vermesine izin vermektedir ancak hizmet sağlayıcısının ABD veya az sayıda başka ülkede yerleşik olmadığı durumlarda, ifşanın yasal temeli ek bir pratik güçlük yaratabilmektedir.

2.4.5 Talep Kapsamı

Çoğu çok uluslu hizmet sağlayıcısı, kapsamı çok geniş olan bilgi taleplerini reddedecektir. Kabul edilebilir kapsam tanımı, “aşırı geniş veya muğlak talepler işlenmeyecektir” ifadesi dışında, genellikle sağlanmamaktadır. Bu nedenle, olumlu bir yanıt almak için en fazla şansa sahip olmak adına, talepler, mümkün olduğunca dar bir kapsamda hazırlanmalı ve mümkün olan durumlarda, söz konusu hususi platformda hangi benzersiz tanımlayıcı kullanılıyorsa onun yardımıyla dava konusu hesaplara atıfta bulunulmalıdır.

Belirli bir platformda hangi eşsiz tanımlayıcının kullanıldığı her zaman açık olmayabilir. Her zaman olmasa da pek çok örnekte, belirli bir hesapla ilişkilendirilen kullanıcı adı ve/veya e-posta adresi yeterli olmaktadır.

2.4.6 Talep Konusunun Bildirilmesi

Pek çok örnekte, çok uluslu bir hizmet sağlayıcısı kullanıcısı ile ilgili bir kolluk talebi alındığında, talebin varlığına ilişkin olarak talebin konusu olan kişiyi bilgilendirmek hizmet sağlayıcısının politikası olmaktadır. Bildirim kanunen veya mahkeme emri tarafından yasaklanmadığı sürece bu yapılacaktır.

Bu nedenle, eğer şahsa bildirim yapılması soruşturmanın gizliliğini ihlal edecekse, hizmet sağlayıcısına gönderilen bilgi talebinin temelini oluşturan formlar, şahsın talep konusunda bilgilendirilmesine dönük yasaklama içermelidir.

Ek olarak, bazı hizmet sağlayıcıları, eğer bir kolluk talebi, hizmet şartlarının sürmekte olan bir ihlaline dikkat çekerse, kullanıcıyı hizmet sağlayıcısının davranıştan haberdar olduğu konusunda bilgilendiren önlemler de dâhil olmak üzere, daha fazla suiistimale engel olmak adına önlem alınabileceğini ifade etmektedir.

ÜZERİNE DÜŞÜNÜLECEK SORULAR

1. Kanıtları ifşa etmek için resmi belgelerin alınması beklenirken, bir ceza yargılamasında, bir hizmet sağlayıcısına gerekli verileri muhafaza etmesi emrini ayrıca vermek neden önemlidir?
2. Bir hizmet sağlayıcısını o hizmet sağlayıcısının bir kullanıcısına ait bilgileri

⁴⁰Bkz. Bölüm 4.2.2.2.2

ifşa etmeye zorunlu kılan bir emrin hizmet sağlayıcısının, talebin konusunu (doğrudan veya dolaylı olarak) bildirmesini engellemeye dönük bir hüküm içerebilmesi için hangi koşulların yürürlükte olması gerekmektedir?

3. Çok uluslu bir hizmet sağlayıcısının bir hesabının sizin yargı yetkisi alanınızdaki suç faaliyetiyle bağlantılı olduğunun bilindiği, fakat hizmet sağlayıcısından bilgi almadan, söz konusu hesabın sahibinin sizin yargı yetkisi alanınızda olup olmadığını bilmenin mümkün olmadığı bir senaryoda, hangi seçeneklerden söz edilebilir?
4. Hukuki yardımlaşma sürecindeki gecikmeler göz önünde bulundurulduğunda, çok uluslu bir hizmet sağlayıcısı tarafından tutulan içerik verilerine erişimi hızlandırmak konusunda ne türden seçenekler (eğer varsa) mevcuttur?

3 Mali Soruşturmalar

3.1 Giriş

İnternet kaynaklı suç gelirlerini hedef alma fikri; hem suçlunun kovuşturulması hem de suç gelirlerinin hedef alınması ve müsadereyi bakış açısıyla, ceza soruşturmaları ile ceza kovuşturmalarının verimliliğini ve başarısını artırmak amacıyla, siber suç soruşturmaları, mali soruşturmalar ve kara para aklama soruşturmalarına ilişkin yaklaşımları bir araya getirmektedir.

Temel eğitim el kitabı mali soruşturmalara ilişkin olarak, kapsam ve unsurlarını da kapsayacak bir biçimde temel ve detaylı açıklamalar içermektedir. Mali soruşturmaların tanımı, aynı zamanda unsurları ve siber suç soruşturmaları da dâhil olmak üzere internet suçlarına ilişkin kimi ayrıntılar kısaca ele alınacak ve AB'de mali soruşturma kavramının son dönemdeki gelişimi hakkında daha fazla detay verilecektir.

3.2 Mali Soruşturmalar ve İnternet Suç Gelirleri

Mali soruşturmanın birden fazla anlamı olabilir; mali suçların araştırılmasından tutun, örneğin, vergilendirme amaçlı araştırmalara kadar çeşitli anlamları olabilir. Uluslararası yasal araçlar mali soruşturma için bir tanımlama getirmemektedir, ancak suç gelirlerinin dondurulması ve müsadereyi çerçevesinde, Mali Eylem Görev Gücü (MEGG) tarafından sağlanan tanımlama örnek olarak kullanılabilir.

Mali soruşturma teriminin ceza yargılaması çerçevesinde suç gelirlerinin hedef alınmasına yönelik soruşturmaları olduğu kadar, (ayrı) medeni (aynı) yargılama çerçevesini de içerebileceği ayrıca not düşülmelidir. Mali soruşturmaların kara para aklama soruşturmaları ile çakışabileceği, ancak ille de çakışması gerekmeyeceği de belirtilmelidir.

Mali soruşturma bir soruşturma yöntemi olup suç gelirlerinin nihai olarak müsadere edilmesi hedefiyle takip edilmesi ve dondurulması ana (fakat münhasır olmayan) amacıyla, kar getiren bir suçun ceza yargılamasına paralel olarak veya hatta adli süreçte mali soruşturma yürütülmesi gerekmektedir.

MEGG mali soruşturmayı⁴¹ bir suç faaliyeti ile ilgili olarak mali işleri konu alan bir tahkikat olarak tanımlamıştır. Burada amaç:

- Suç ağlarının kapsamını ve suçun ölçeğini saptamak,
- Suç gelirlerini, terör para kaynaklarını veya müsadereye konu olan ya da olabilecek diğer tüm varlıkları saptamak ve bunların izini sürmek,
- Ceza kovuşturmalarında kullanılacak kanıtları geliştirmektir.

Suç kaynaklı karlar en azından kısmen yasallaştırılma ve yasal ekonomide yeniden kullanılma eğiliminde olduğu için, mali soruşturmalar kara para aklama soruşturmaları ile ilişkili olabilir ve/veya bunlara yol açabilir. Mali soruşturma bir kara para aklama suçu şüphesine yol açabilir veya alternatif olarak bir mali istihbarat birimi (MİB) şüpheli işlemleri analiz ederken veya kara para aklama suçunu soruştururken, (müsnet) suç kaynaklı

⁴¹MEGG (2012), Tavsiye 30'a Yorumlayıcı Not, 2. paragraf.

Ayrıca bkz.: Operasyonel konularla ilgili MEGG Raporu. Mali soruşturma kılavuzu, 2012.

gelirler müsadere konusu haline gelebilmektedir (bir kara para aklama suçu konusu olarak).

3.2.1 Mali Soruşturma Unsurları

Mali soruşturma, en iyi, unsurları⁴² tanımlanarak ve pratikte uygulanacak uluslararası ve ulusal ilgili kanuni hükümler saptanarak tanımlanabilir.

Temel eğitimde anlatıldığı gibi, bir mali soruşturmanın unsurları şunlardır:

1. Suçun ve failin saptanması (ceza soruşturmasına paralel olarak)
2. Suç gelirlerinin (değerinin) tespiti
3. Müsadere edilebilir mülklerin tespiti
4. Dondurma emri; müsaderenin güvence altına alınmasına yönelik geçici önlemler

Bir mali soruşturmanın ve potansiyel olarak bir dondurma emrinin sonucu suç gelirlerinin nihai müsaderesi olacaktır.

3.2.2 Mali Soruşturmanın Siber Suç ile ilgili Yönleri

Temel eğitimde daha detaylı bir biçimde sunulduğu üzere, mali soruşturmanın dört unsuru siber suç ve/veya internet suçu soruşturmalarında da uygulanabilmektedir ki bunlar internet üzerinden elde edilen suç gelirlerini de içermektedir.

İnternet suçlarının soruşturulması ile ilgili, göz önünde bulundurulması gereken bazı ayrıntılar bulunmaktadır:

- Fail kimdir ve suç kanıtları nerededir?
 - Bu soru; İP adresi, abone verilerine erişim, elektronik iletişim veya sosyal ağ verileri ve potansiyel olarak akış ve içerik verileri kullanılarak bir şüphelinin saptanması, gerek ulusal gerek uluslararası İSS'ler ile işbirliği, verilerin muhafazasına yönelik talepler ile elektronik kanıtlara el konulması ve bunların çıkarılmasına yönelik mahkeme emirlerinin oluşturulması ile ilişkilidir.
- Suç gelirleri nedir?
 - Bu soru; e-para, sanal para birimleri (örneğin Bitcoin) ve internet bankacılık ödemeleri türünden varlıklar ile ödeme sistemleri, yurtdışında yer alan banka hesapları, muhtemelen fonların kaynağını gizlemek üzere yapılandırılan farklı tipte çoklu işlemler, kara para aklama tiyolojileri ile ilişkilidir.
- Ne müsadere edilebilir/bir şüphelinin mal varlığı?
 - İnternet üzerindeki para akışları düşünüldüğünde, yargı yetkisi alanına dair de bir soru ortaya çıkmaktadır. Mağdurlar ve failer genelde aynı ülkede olmamaktadır. Mali soruşturma ya da kara para aklama yaklaşımı üzerinden siber suç gelirlerinin müsadere edilmesi düşünülmelidir. Odak noktası ve hedef; en azından suçtan doğrudan elde edilen gelirler (ödenen harağlar veya dolandırıcılık işlemleri) ve suçlarda kullanıldığı saptanan banka hesaplarının dondurulması (internet üzerinden harağ, bilgisayar dolandırıcılığı) olmalıdır.

⁴²Daha fazla detay için bkz. Temel Eğitim El Kitabı (1.1.3).

- Siber suç soruşturmalarında paralel olarak mali soruşturma yürütülmesi, failin gelirlerinin (banka hesapları ve para akışı, sanal para transferleri) ve mevcut mal varlığının saptanması açısından önemlidir.
- Dondurma emri
 - E-bankacılık ve genel olarak internet söz konusu olduğunda hızlı hareket etmek son derece önemlidir. Kara para aklama suçlarının araştırılması ve Mali İstihbarat Birimi yetkilerinin ve uluslararası bağlantılarının kullanılması olası bir çözüm olabilmektedir. Süreci hızla mahkeme emri ve hukuki yardımlaşma izlemelidir. Hukuki yardımlaşma için INTERPOL kanalının kullanılması, Varşova Sözleşmesi ve Budapeşte Sözleşmesi'nin getirdiği ek olanaklar, ikili anlaşmalar ve karşılıklılık yaklaşımı göz önünde bulundurulmalıdır.
- Müsadere
 - Farklı müsadere rejimleri ve varlık paylaşımı ile alakalı olarak hukuki yardımlaşma konusunda uluslararası davalarda sorular ortaya çıkmaktadır.

3.2.3 Avrupa Birliği'nde Mali Soruşturma

AB'nin 2016 Hollanda başkanlığı dönemi, suç gelirlerinin hedef alınması ile mali soruşturmaları, önceliklerinden birisi olarak belirlemiştir. Avrupa Birliği'nde mali soruşturma araç ve yöntemlerine ilişkin bir ihtiyaç değerlendirmesinin yanı sıra "mali soruşturma konusunda bilinmesi gereken altı şey" broşürü da hazırlanmıştır⁴³.

İhtiyaç değerlendirmesi⁴⁴ şunların altını çizmiştir:

- **Mali soruşturma, suç yaratan her türlü geliri konu alabilir:** Kara para aklama da dâhil olmak üzere mali/ekonomik suçlarla mücadele veya esas itibarıyla varlıkların geri alınması için kanıt toplanması ile sınırlı değildir.
- **Mali soruşturma, ceza soruşturmaları ile adli muamelelerin tüm aşamalarında yürütülmelidir:** suçun saptanması, istihbarat geliştirilmesi, kanıtların toplanması aşamalarından kovuşturma, mahkûmiyet ve varlık müsaderesi aşamalarına kadar.

"Mali soruşturma konusunda bilinmesi gereken altı şey" broşüründe de vurgulandığı gibi, suç işlemekteki temel motivasyon çoğu zaman finansal kar olduğundan, gelirler sıklıkla meşru şirketler ve yardımcı kuruluşlar kullanılarak mallara harcanmakta ve ekonomide aklanmaktadır. Mali soruşturma, kolluk araçları içerisinde ek bir soruşturma aracıdır ve bir suç örgütü içerisindeki lider bireyleri hapse atıp onların para ve varlıklarını almakta kullanılabilir. Lider kişileri mali durumlarından yoksun bırakmak onların suç faaliyetlerini sürdürmesini çok zorlaştıracaktır. Bu da mali soruşturmaları organize suçlar ve terörizmi akamete uğratmakta son derece etkili bir araç haline getirmektedir.

"Bilinmesi gerekenler" broşürü ayrıca şunların altını çizmektedir:

- **Mali soruşturma, her çeşit suça uygulanabilmektedir:** Mali soruşturma, insan kaçakçılığı - kaçakçılık, dolandırıcılık, uyuşturucu ve silah kaçakçılığı ve

⁴³Broşür: Mali soruşturma konusunda bilinmesi gereken altı başlık, Şubat 2016. Ulaşmak için bkz.: <https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>

⁴⁴Avrupa Birliği'nde mali soruşturma araç ve yöntemlerine ilişkin ihtiyaç değerlendirmesi, ECORYS, Aralık 2015. Ulaşmak için bkz.: https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf

terörizm gibi her türlü ciddi ve organize suça uygulanabilir ve uygulanmalıdır. Mali soruşturmanın dolandırıcılık, vergi suçları, yolsuzluk ya da kara para aklama gibi ekonomik suçlar ile mücadeleyle sınırlı olduğu genel bir yanlış kanıdır.

- **Ceza kovuşturmalarına eşlik eden mali soruşturmalar:** İdeal olarak, mali soruşturmalar, ceza soruşturmaları ile adli muamelelerin her aşamasında uygulanmaktadır. Suç veya suç ağlarının proaktif bir şekilde saptanmasından turun, dava soruşturmalarına ve kanıtların toplanmasına kadar; suçluların kovuşturulması ile mahkûm edilmesinden mal müsaderesine kadar. Ancak pek çok örnekte, mali soruşturma görevlileri, suç gelirlerini izlemek, saptamak ve müsadere etmek üzere ceza soruşturmalarına ancak son aşamada dâhil edilmektedirler. Bu fırsat kaçırılması anlamına gelmektedir. Mali soruşturmalar mümkün olan en erken şekilde başlamalıdır.
- **Geniş kapsamlı finansal farkındalık çok önemlidir:** Kolluk sisteminin tüm düzeylerinde mali farkındalığa ihtiyaç duyulmaktadır; mahalli polis teşkilatı düzeyindeki temel finansal farkındalıktan tutun, karmaşık sınır ötesi kara para aklama yapılarının arkasındaki "kurumsal örtü"yü kaldırmak için ihtiyaç duyulan son derece uzmanlaşmış adli muhasebe uzmanlığına kadar. Ceza işleri soruşturma görevlilerinin, bir suç mahallinde mali kanıt toplama ve gerektiğinde özelleşmiş mali uzmanları çağırma ihtiyacının farkında olmaları önem taşımaktadır. Ayrıca, mali soruşturma görevlileri tarafından hazırlanan dosyaları anlamak ve değerlendirmek bakımından savcı ve hâkimler arasındaki mali uzmanlık çok önemlidir.
- **Mali soruşturmalarda başarının anahtarı sınır ötesi işbirliğidir:** Soruşturma görevlileri soruşturmaları sürdürmek için enformel bilgi alışverişi yollarına (CARIN, Europol, INTERPOL) olduğu kadar hukuki yardımlaşma talepleri türünden formel yollara da aşına olmalıdır.
- **Çok disiplinli işbirliğinin önemi:** En iyi sonuçlar; kolluk kuvvetleri, savcılar, Mali İstihbarat Birimleri (MİB) ve vergi makamları gibi mali soruşturmalara dâhil olan kamu görevlileri uzmanlıklarını birleştirdiklerinde, birlikte çalışarak bilgi paylaştıklarında ortaya çıkmaktadır. Dahası, bankalar, emlak ofisleri ve diğer profesyonel hizmet sağlayıcıları gibi özel sektör taraflarının mali soruşturmalarda değerli girdiler sağlayabildikleri ve sağlamaları gerektiği yönünde giderek artan bir bilinç ve isteklilik oluşmuştur.

ÜZERİNE DÜŞÜNÜLECEK SORULAR

1. Bir mali soruşturmanın bir siber suç soruşturmasına paralel olarak yürütülmesini engelleyebilecek, eğer varsa, ne tür pratik veya yasal engeller öngörebilirsiniz?
2. İnternet veya sanal biçimlerde tutulan suç gelirlerinin saptanmasını engelleyebilecek, eğer varsa, ne tür pratik veya yasal engeller öngörebilirsiniz?
3. Ceza kovuşturmalarında hangi noktada (soruşturma, adli süreç vs.) bir mali soruşturma başlatılabilir?
4. Malların dondurulmasına yönelik bir emir verilebilmesi için hangi koşulların gerçekleşmesi gerekmektedir?

4 Sınır Ötesi İşbirliği

4.1 Özet

İnternet, olumlu yanlarıyla birlikte, kimliklerini, suç kaynaklı gelirlerin kanıtlarını ve izlerini gizleyerek neredeyse görünmez yollardan, hızla ve imzasız şekilde hareket edebilen suçlulara istismar olanakları sunmaktadır. Bu özellik, kolluk kuvvetleri açısından bir güçlüğü temsil ediyor.

İnternet kaynaklı suç gelirleri soruşturmalarının üç yönünü birleştirmek yoluyla gerçekleştirilecek farklı işbirliği olasılıklarının faydalarını anlamak önem taşımaktadır: siber suç soruşturmaları, paralel mali soruşturmalar ve kara para aklama soruşturmaları⁴⁵. Avrupa Konseyi Varşova Sözleşmesi ve Budapeşte Sözleşmesi bu yönlerin ele alınmasında önemli araçlardır.

Temel eğitim; uluslararası işbirliğinin başlıca yönlerini, siber suç ve elektronik kanıtlar konusunu, ayrıca mali soruşturma ve kara para aklamanın önlenmesi ve soruşturulması alanlarında uluslararası işbirliği yollarını birleştirmenin avantajlarını içermekte, (operasyonel) bilgilerin değiş tokuşunu içeren uluslararası işbirliğini, kanıtlara yönelik hukuki yardımlaşma, bilgi değiş tokuşuna yönelik ilgili uluslararası ağlar ve kuruluşlar, Budapeşte ve Varşova sözleşmelerinin ilgili hükümleri üzerinden ele almaktadır.

Ayrıca, uluslararası işbirliğine ve özellikle hukuki yardımlaşmaya ilişkin göz önünde bulundurulması gereken bazı zorluklar söz konusudur.

Budapeşte ve Varşova Sözleşmeleri, paralel (siber) suç soruşturmaları ile mali soruşturmalar birleştirilirken uygulanacak olan uluslararası işbirliği yollarını tanıtmaktadır. Bununla birlikte, uluslararası işbirliği, elektronik kanıtların doğası, bulut teknolojisi, aynı zamanda taraflar arasındaki farklı müsadere rejimleri ve hukuki farklılıklar dikkate alındığında, suç gelirlerinin belirlenmesi, yurtdışındaki mülklerin zapt edilmesi ve müsadere gibi pratik şartların bir sonucu olan, sözleşmelerin her birisine ait özel hukuki ve pratik zorluklarla karşı karşıyadır. Bu zorluklar, Cezai Meselelerde İşbirliğine Dair Avrupa Sözleşmelerinin İşleyişinden Sorumlu Uzmanlar Komitesi (PC-OC) ve Siber Suçlar Sözleşmesi Komitesi gibi ilgili Avrupa Konseyi organlarınca tespit edilmiş ve ele alınmıştır.

Siber suç soruşturmaları, mali soruşturmalar ve kara para aklamanın önlenmesi ve soruşturulması süreçleri birleştirilirken, tüm bu farklı yönlerin, Budapeşte ve Varşova sözleşmelerinin önerdiği işbirliği yollarının faydaların ve mevcut zorlukların farkında olmak yarar taşımaktadır.

Hukuki yardımlaşma halen yurtdışında mahkeme kararlarının icrası ve kanıtların toplanması açısından temel araç kabul edilirken, prosedürün uzunluğu önemli bir engel oluşturmaktadır. Ancak, ortak soruşturmaların ve ortak soruşturma ekiplerinin kullanılması, verimlilik ile ilişkili bazı zorlukları karşılayabilmektedir. Kolluk kuvvetleri (polis ve savcı) arasındaki işbirliği ve bilgi alışverişi sınır ötesi davalarda vazgeçilmezdir. İlgili uluslararası ağlar ve kuruluşlar, bu bakımdan önemli bir rol oynamakta ve ayrıca güven inşasına yardım etmektedirler. Bunlar tarafından sunulan işbirliği kanalları ve araçları, suç soruşturmalarında bilgi ve kanıt alışverişi açısından esastır.

⁴⁵ Ancak, muhtelif ülkelerdeki olası önleme ve mücadele araçlarına karşın, kara para aklama soruşturması, hala zorlu bir görev.

4.1.1 Bilgi Alışverişine ve Hukuki Yardımlaşmaya Yönelik İlgili Ağlar ve Örgütler

Uluslararası İşbirliği – (Operasyonel) Bilgi Alışverişi Polisten polise, savcıdan savcıya	
7/24 Ağ	Ağ (polis ve/veya savcı iletişim noktaları) Budapeşte Sözleşmesi 35. maddesi
EGMONT	MİB'ler ağı; kara para aklama önleme, şüpheli işlemlerin ertelenmesi. Varşova Sözleşmesi 46. maddesi
CARIN	Varlık Geri Edinimi Kurumlar Arası Ağı Suç gelirleri müsadere uzmanları ağı
INTERPOL	Bilgi alışverişi ve hukuki yardımlaşma talepleri iletim kanalı
Europol (EC3)	AB ve AB üyesi olmayan ülkelerle yapılan ilgili anlaşmalar
Eurojust	Avrupa Siber Suçlar Yargı Ağı (2016) AB ve AB üyesi olmayan ülkelerle yapılan ilgili anlaşmalar
Uluslararası İşbirliği – Hukuki Yardımlaşma Resmi işbirliği - kanıtlar	
Hukuki yardımlaşma: Resmi işbirliği, hukuki yardımlaşma talebinin sonucu mahkemede kanıt olarak kullanılabilir. Olağan iletişim kanalları, atanmış merkezi makamları içermektedir, bunlar çoğu zaman Adalet Bakanlığı veya Dışişleri Bakanlığı'dır.	
Doğrudan işbirliği: Hâkimden hâkime, savcıdan savcıya (AB, iki taraflı anlaşmalar) Varşova (Madde 34) ve Budapeşte (Madde 27/9) sözleşmeleri de merkezi makamlar üzerinden iletilen resmi talep yoluyla, acil durumlarda, sorumlu adli yetkililer ve kovuşturma yetkilileri arasında doğrudan işbirliği yapılmasını öngörmektedir.	
Diğer seçenekler	Ortak Soruşturma Ekipleri Paralel soruşturma Gelir aktarımı

Suçlular, mülklerini yurtdışında saklarlar (veya tutarlar). Uluslararası suç gruplarının işlediği suçların soruşturulmasında, failerin yurtdışında mülklerinin bulunup bulunmadığının doğrulanması önemlidir. Bu tip durumlarda, **polis ve savcı işbirliği** çok önemlidir. Yabancı büroda iletişim kurulacak bir kişi; polis işbirliği veya istinabe müzekkeresi ile kamu kaynaklarından mülk hakkında hangi verilerin elde edilebileceği konusunda tavsiyede bulunabilir. Bu tür bilgiler, verilerin elde edilmesini kayda değer ölçüde kolaylaştırıp hızlandırabilmektedir. Bu tür işbirlikleri operasyonel olup mahkeme kararlarının uygulanması kapsam dışıdır.

Operasyonel temaslar ve işbirliği, ilkesel olarak, daha etkin bir hukuki yardımlaşma yaklaşımını ortaya koyacak olan ortak soruşturma ekiplerinin kurulmasını da sağlayabilmektedir. Ayrıca, daha fazla sayıda fail ve mağdur içeren sınır ötesi davalarda paralel soruşturmaların düzenlenmesini sağlayabilmektedir.

Hukuki yardımlaşma resmi işbirliğidir ve talebin sonucu mahkemede kanıt olarak kullanılabilir. Olağan iletişim kanalları atanmış merkezi makamları içermektedir, bunlar çoğu zaman Adalet Bakanlıkları olmaktadır. Diğer olası kanallar Dışişleri Bakanlığı veya acil durumlarda INTERPOL, Europol veya Eurojust olabilir.

AB içerisinde hukuki yardımlaşma, doğrudan sorumlu makamlar (savcı/mahkeme) arasında işlemektedir. Varşova (Madde 34) ve Budapeşte (Madde 27/9) sözleşmeleri de acil durumlarda merkezi makamlar üzerinden aktarılan resmi talepleri içeren bu türden yaklaşımları öngörmektedir.

4.1.2 Uluslararası Hukuki Araçlar

Siber Suçlar	Mali Soruşturmalar
Avrupa Konseyi	
Budapeşte Siber Suçlar Sözleşmesi ve Yabancı Düşmanlığı ve Irkçılık Hakkında Protokol ⁴⁶	Suç Gelirlerinin Aklanması, Zapt Edilmesi ve Müsaderesi ve Terörizmin Finanse Edilmesi Hakkında Varşova Sözleşmesi ⁴⁸
Siber Suçlar Sözleşmesi Komitesi Kılavuz Notları ⁴⁷	1990 Suç Gelirlerinin Aklanması, Aranması, Zapt Edilmesi ve Müsaderesi Konulu Strazburg Sözleşmesi ⁴⁹
AB	
Bilgi sistemlerine karşı saldırıları konu alan, 12 Ağustos 2013 tarihli, 2013/40/EU sayılı Avrupa Parlamentosu ve Konsey Direktifi ve 2005/222/JHA sayılı, değiştiren Konsey Çerçeve Kararı ⁵⁰	Avrupa Birliği'nde suç vasıtaları ve gelirlerinin dondurulması ve müsaderesi hakkında, 2014/42/EU sayılı Direktif ⁵¹
Ağ ve bilgi sistemlerinde yüksek bir ortak güvenlik seviyesine dönük önlemleri konu alan, Temmuz 2016 tarihli, 2016/1148 sayılı Avrupa Parlamentosu ve Konsey Direktifi (NIS Direktifi) ⁵²	Kara para aklama, suç vasıtaları ve gelirlerinin saptanması, izlenmesi, dondurulması, zapt edilmesi ve müsaderesi konulu, 98/699/JHA sayılı Ortak Eylem ⁵³

⁴⁶ Siber Suçlar Sözleşmesi, ETS 185, 21.11.2001 ve Bilgisayar sistemleri üzerinden işlenen, ırkçı ve yabancı düşmanı nitelikli eylemlerin suç olarak kabul edilmesine ilişkin, Siber Suçlar Sözleşmesi Ek Protokolü, ETS 189, 28.01.2003.

⁴⁷ <https://www.coe.int/en/web/cybercrime/guidance-notes>

⁴⁸ Suç Gelirlerinin Aklanması, Zapt Edilmesi ve Müsaderesi ve Terörizmin Finanse Edilmesi Hakkında Sözleşme, CETS 198, 16.05.2005.

⁴⁹ Suç Gelirlerinin Aklanması, Aranması, Zapt Edilmesi ve Müsaderesi Konulu Sözleşme, Strazburg, ETS 141, 08.11.1990.

⁵⁰ Direktif bilgi sistemlerine dönük bir dizi suç için suç kabul edilme şartlarını ve cezaları uyumlaştırıcı yeni kurallar getirmektedir. Ayrıca, AB ülkelerine ileri teknoloji içeren tehditlere hızla reaksiyon göstermek üzere, Avrupa Konseyi ve G8 tarafından kullanılan iletişim noktalarının ayınlarını kullanma çağrısında bulunmaktadır. Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>

⁵¹ Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042>

⁵² NIS Direktifi Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2016.194.01.0001.01.ENG>

⁵³ Organize suçlarla mücadele alanında Avrupa Birliği (AB) ülkeleri arasındaki işbirliğini iyileştirmek üzere, bu ortak eylem, Avrupa Yargı Ağı operasyonları kapsamında, suç vasıtaları ve gelirlerinin saptanması, izlenmesi, dondurulması veya zapt edilmesi ve müsaderesi ile ilgili kullanıcı dostu kılavuzların hazırlanmasını öngörmektedir. Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=uriserv%3A33073>

Siber uzayda ceza yargılamasının iyileştirilmesi konulu Avrupa Birliği Konsey Sonuçları ile Avrupa Siber Suçlar Yargı Ağı konulu Sonuçlar ⁵⁴ , Haziran 2016	Kara para aklama, suç vasıtaları ve gelirlerinin saptanması, izlenmesi, dondurulması, zapt edilmesi ve müsadere konulu, 2001/500/JHA sayılı Konsey Çerçeve Kararı ⁵⁵
	Mali sistemin kara para aklama veya terörizmin finansmanı amaçlarıyla kullanılmasının önlenmesi hakkında, 2015/849 sayılı Direktifi değiştiren 2009/101/EC sayılı Direktif ⁵⁶
	Suç bağlantılı gelirler, vasıtalar ve mülklerin müsadere konulu, 2005/212/JHA sayılı Çerçeve Kararı ⁵⁷
	Malları veya kanıtları donduran emirlerin Avrupa Birliği'nde uygulanması hakkında, 2003/577/JHA sayılı Çerçeve Kararı ⁵⁸
	Müsadere emirlerinin karşılıklı olarak tanınması ilkesinin uygulanması hakkında, 2006/783/JHA sayılı Çerçeve Kararı ⁵⁹
	Suç gelirlerinin veya suçla ilişkili diğer mülklerin izlenmesi ve saptanması alanında Üye Devletlerin Varlık Geri Kazanımı Daireleri arasındaki işbirliğini konu alan, 2007/845/JHA sayılı Konsey Kararı (Varlık Geri Kazanımı Ofis(ler)i kurulması yükümlülüğünü getirmiştir) ⁶⁰

⁵⁴Sonuçlar şunlara odaklanmaktadır: verilerin hızla ifşa edilmesine izin verecek şekilde hizmet sağlayıcıları ile işbirliği kurulması; belirli veri kategorilerinin, özellikle de abone verilerinin elde edilmesi için daha az sıkı yasal süreçler öngörülebilir. Elektronik verilerle ilgili hukuki yardımlaşma prosedürleri hızlandırılmalı ve kolaylaştırılmalıdır; hizmet sağlayıcıları ile işbirliğini genişletmek yoluyla yetkili makamlar arasındaki hukuki yardımlaşma talepleri hacmi azaltılabilir. E-kanıtları etkin şekilde güvence altına alınması ve elde edilmesini temin etmek için, karşılıklı tanıma prosedürleri verimli şekilde kullanılmalıdır. Verilerin yerinin (henüz) bilinmediği ya da uçucu olduğu örneklerde, siber uzayda yargı yetkisi alanı uygulamaya yönelik bağlayıcı faktörlerin oluşturulması. Ulaşmak için bkz.: <http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/>.

⁵⁵Kara para aklama, suç vasıtaları ve gelirlerinin saptanması, izlenmesi, dondurulması, zapt edilmesi ve müsadere konulu, 26 Haziran 2001 tarihli, 2001/500/JHA sayılı Konsey Çerçeve Kararı (Resmi Gazete L 182, 5.7.2001, s.1). Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>

⁵⁶Takas hizmetleri ve emanet cüzdan sağlayıcılarının Ulusal Mali İstihbarat Birimi (MİB) ile bu meyanda işbirliğinde bulunmasını zorunlu kılarak sanal para birimlerini düzenlemeyi de amaçlamaktadır. Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0450:FIN%20>

⁵⁷Suç bağlantılı gelirler, vasıtalar ve mülklerin müsadere konulu, 24 Şubat 2005 tarihli, 2005/212/JHA sayılı Konsey Çerçeve Kararı (Resmi Gazete L 68, 15.3.2005, s.49). Ulaşmak için bkz.: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>

⁵⁸Avrupa Birliği'nde mülkleri veya kanıtları dondurma emirlerinin uygulanması konulu, 22 Temmuz 2003 tarihli ve 2003/755/JHA sayılı Konsey Çerçeve Kararı (Resmi Gazete L 196, 2.8.2003, s.45). Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>

⁵⁹Müsadere emirlerinin karşılıklı olarak tanınması ilkesinin uygulanması hakkında, 6 Ekim 2006 tarihli, 2006/783/JHA sayılı Konsey Çerçeve Kararı (Resmi Gazete L 328, 24.11.2006, s.59). Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>

⁶⁰Karar AB ülkelerinde ulusal Varlık Geri Kazanımı Ofisleri kurulmasına yönelik şartları tespit etmektedir. Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>

	Cezai konularda Avrupa Soruşturma Emri konulu, 2014/41/EU sayılı Direktif ⁶¹
BM	
Bilgi Teknolojilerinin Suç Oluşturacak Şekilde istismar Edilmesi ile ilgili Kararlar (55/63 ve 56/121 sayılı Kararlar) ⁶²	1988 Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı Birleşmiş Milletler Sözleşmesi ⁶³
Küresel bir siber güvenlik kültürü yaratılması ile ilgili, 64/211 sayılı BM Genel Kurul Kararı (Mart 2010) ⁶⁴	2000 Sınır Aşan Organize Suçlara Karşı Birleşmiş Milletler Sözleşmesi ⁶⁵
	2003 Birleşmiş Milletler Yolsuzlukla Mücadele Sözleşmesi ⁶⁶
Diğerleri (bölgesel anlaşmalar)	
Siber Güvenlik ve Kişisel Verilerin Kullanımı konulu Afrika Birliği Sözleşmesi ⁶⁷	
Bilgi Teknolojisi Suçları ile Mücadele konulu Arap Sözleşmesi ⁶⁸	
Bilgisayar Bilgileri ile ilgili Suçlarla Mücadelede İşbirliği konulu Bağımsız Devletler Topluluğu Anlaşması ⁶⁹	
Uluslararası Bilgi Güvenliği Alanında Shanghai İşbirliği Örgütü Anlaşması ⁷⁰	

AB içerisinde, 2003'ten itibaren dondurma kararlarının uygulanışında ve 2006'da müsadere kararları için, yardımlaşma karşısında, karşılıklı tanıma ilkesi getirilmiştir. Uygulamayı ret kapsamı, ayrıca, her iki tarafta da suç olarak kabul edilme ve her iki tarafta da dondurma ilkelerinin istisnalarıyla sınırlandırılmıştır. AB Avrupa Soruşturma Emri'ni getirerek işbirliğini kolaylaştırıcı başka adımlar da atmıştır.

4.1.3 Uluslararası İşbirliği Hükümleri

Uluslararası hukuki araçlar, hukuki yardımlaşma için yasal zemin de dâhil olmak üzere davranışın suç kabul edilmesi, usul (soruşturma araçları) ve uluslararası işbirliği konularıyla ilgilenmektedir. Varşova ve Budapeşte sözleşmeleri, paralel mali ve (siber) suç

⁶¹Avrupa Soruşturma Emri direktifi, birden fazla ülkenin dahil olduğu ceza davalarında, AB ülkelerinin diğer AB ülkelerinde kanıt elde etmesine izin veren, kapsamlı, yeni bir sistem oluşturmaktadır. Ulaşmak için bkz.: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>

⁶²Ulaşmak için bkz.: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

⁶³Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı Birleşmiş Milletler Sözleşmesi, Viyana, 19.12.1988 (Madde 5).

⁶⁴Ulaşmak için bkz.: <https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf>

⁶⁵Sınır Aşan Organize Suçlara Karşı Birleşmiş Milletler Sözleşmesi, New York, 15.11.2000 (12-14. maddeler).

⁶⁶Birleşmiş Milletler Yolsuzlukla Mücadele Sözleşmesi, New York, 31.10.2003 (31, 54-57. maddeler).

⁶⁷<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

⁶⁸http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences

⁶⁹http://itlaw.wikia.com/wiki/Agreement_on_Cooperation_Among_the_States_Members_of_the_Commonwealth_of_Independent_States_in_Combating_Offences_Relating_to_Computer_Information

⁷⁰<https://ccdcoe.org/sco.html>

soruşturmaları gerçekleştirilirken en etkili neticelerin elde edilmesini sağlamak üzere kullanılabilir ve birleştirilebilecek yollar öngörmektedir. İşbirliği; taleplerin ertelenmesi ve reddine yönelik emniyet tedbirleri içeren ulusal hükümlere tabidir (Varşova Sözleşmesi Bölüm 5, Madde 27 ve Budapeşte Sözleşmesi, Madde 25/4, 27/4 ve 5). Temel işbirliği alanları aşağıda gösterilmektedir:

Uluslararası İşbirliği Hükümleri	
Budapeşte Sözleşmesi	Varşova Sözleşmesi
Temel İlkeler	
<p>(23-25. maddeler)</p> <p>Taraflar, şunlarla ilgili olarak, soruşturma ve kovuşturmalarda karşılıklı yardım sağlayacaktır:</p> <ul style="list-style-type: none"> - siber suçlar (2-10. maddeler) veya - bir suçla ilgili olarak elektronik kanıt toplanması 	<p>(15. madde)</p> <p>Taraflar, vasıtaların ve gelirlerin müsadereğini amaçlayan soruşturma ve kovuşturmalarda karşılıklı işbirliği sağlayacaktır.</p> <p>Talepler:</p> <ul style="list-style-type: none"> - belli malların müsadere veya - gelirlerin değerine denk gelen bir miktarın ödenmesi ve - müsadere maksadıyla soruşturma yardımı yapılması ve geçici tedbirler alınması
Kendiliğinden Bilgilendirme	
<p>(26. madde)</p> <p>Bir Taraf, yerel mevzuatının sınırları çerçevesinde ve ön talep olmaksızın, başka bir tarafa, kendi soruşturmasının çerçevesi içinde edinilen bilgileri, bu bilgilerin ifşasının alıcı tarafa, bu sözleşme uyarınca belirlenen suçlara yönelik soruşturma veya kovuşturma başlatmakta ya da yürütmekte yardımcı olabileceğini veya bu bölüm kapsamında söz konusu taraftan gelecek bir işbirliği talebine yol açabileceğini düşünüyorsa, sağlayabilir.</p>	<p>(20. madde)</p> <p>Benzer hüküm</p>
Geçici Tedbirler	
<p>(29-30. maddeler)</p> <p>Depolanan bilgisayar verilerinin hızlandırılmış muhafazası.</p> <p>Korunan akış verilerinin hızlandırılmış ifşası.</p>	<p>(21-22. maddeler)</p> <p>Mülkiyetin alım satımını, devrini ve elden çıkarılmasını önlemek üzere dondurulması veya zapt edilmesi ve geçici tedbir için ilgili tüm bilgilerin kendiliğinden sağlanması.</p>

Soruşturma Yardımı	
<p>(31-34. maddeler)</p> <p>Soruşturma yetkilerine ilişkin yardımlaşma:</p> <ul style="list-style-type: none"> - Depolanmış bilgisayar verilerine erişim; - Depolanmış bilgisayar verilerine rıza ile veya kamuya açık olduğu durumlarda sınır ötesi erişim; - Akış verilerinin gerçek zamanlı olarak toplanması; ve - İçerik verileri ile ilgili olarak iletişimde araya girme. 	<p>(16-19. maddeler)</p> <p>Taraflar, yukarıda adı geçen mülkün varlığı, yeri veya hareketi, niteliği, yasal statüsü veya değerine ilişkin kanıtların güvence altına alınmasını içerecek şekilde, vasıta ve gelirlerin tespiti ve takibinde yardımlaşacaklardır. Bu yardımlaşma şu talepleri de kapsayacaktır:</p> <ul style="list-style-type: none"> - banka hesap bilgileri; - banka işlem bilgileri; - banka işlemlerinin izlenmesi.
	<p>Müsadere</p>
	<p>(23-25. maddeler)</p> <ul style="list-style-type: none"> - Müsadere kararının uygulanması veya - Yetkili mercilere müsadere emri almak amacıyla talepte bulunmak ve bu talebi, gelirlerin değerine denk bir meblağ ödenmesi veya mülkün belli bir parçasının müsadere edilmesi talebini de içerecek şekilde yürürlüğe konması.
	<p>(Madde 23/5)</p> <p>Müsadere için eşdeğeri olan önlemler:</p> <ul style="list-style-type: none"> - suçla ilgili olmayan yaptırımlar (mahkûmiyete bağlı olmayan müsadere); - varlıkların paylaşılması kuralları (mağdurlara, yasal maliklere telafi).
İşbirliği Ağları	
<p>7/24 Ağ (35. madde)</p> <p>Her Taraf, şu amaçlarla, acil yardım hükümlerini güvence altına almak üzere 7/24 ulaşılabilir bir iletişim noktası belirleyecektir:</p> <ul style="list-style-type: none"> - bilgisayar sistem ve verileriyle ilgili bir suç konu alan soruşturma ve kovuşturmalar veya - bir suç ile ilişkili olarak elektronik kanıtlarının toplanması <p>Söz konusu yardım, aşağıdaki önemleri kolaylaştıracak ya da yerel mevzuatın izin vermesi halinde, bu önlemleri doğrudan uygulayacaktır:</p> <ul style="list-style-type: none"> - teknik tavsiye verilmesi; - verilerin korunması (29 ve 30. maddeler); - kanıtların toplanması, - hukuki bilgi sağlanması, - ve şüphelilerin yerlerinin tespit edilmesi. 	<p>MİB İşbirliği (46-47. maddeler)</p> <p>MİB'ler kendiliğinden veya talep üzerine şunlarla alakalı olabilecek her tür erişilebilir bilgiyi paylaşmaktadır:</p> <ul style="list-style-type: none"> - Bilgilerin işlenmesi veya analizi veya - Kara para aklama ve para aklamaya karışan gerçek veya tüzel kişilerle ilgili mali işlemler konusunda MİB tarafından yürütülen soruşturmalar. <p>MİB'in şüpheli işlemleri erteleme yetkisi.</p>

ÜZERİNE DÜŞÜNÜLECEK SORULAR

1. Bilgilerin bir başka yargı yetkisi alanıyla eş zamanlı olarak paylaşılabilmesi öncesinde hangi koşullar ortaya çıkmalıdır?
2. Uluslararası bir yardım talebiyle işbirliği yapmayı reddetmek için sizin ulusal mevzuatınızda hangi temeller mevcuttur?
3. Muhafaza edilen akış verilerinin ifşasını hızlandırmak adına bir emir çıkarmak için hangi koşulların ortaya çıkması gerekmektedir?
4. Yürürlükte, bir başka yargı yetkisi alanıyla müsadere edilen varlıkların yönetimine, devrine ve paylaşılmasına izin veren hangi pratik önlemler bulunmaktadır? Burada duruma göre mi düzenleme yapılmalıdır?

4.2 Uluslararası İşbirliği Hükümlerinin Uygulanması Hakkında Değerlendirmeler

Mali soruşturmalar ve siber suç soruşturmaları alanındaki uluslararası işbirliği ile ilgili fırsat ve engeller, uluslararası kuruluşlar tarafından tanımlandığı haliyle elektronik kanıtlar hakkında düşünmek ve bunları anlamak önem taşımaktadır.

4.2.1 Suç Gelirlerinin Hedef Alınması Hakkında Değerlendirme

4.2.1.1 GENVAL

AB'de⁷¹ "mali suçlar ve mali soruşturmalar" karşılıklı değerlendirmeleri beşinci raundu bağlamında, Değerlendirmeleri de İçeren Genel Meseleler Çalışma Grubu (GENVAL), 2012 nihai raporunda⁷² bu alana ait kilit nitelikteki güçlüklerin altını çizmiştir, şöyle ki:

1. Dava yönetimi (zaman ve kaynak yönetimi dâhil olmak üzere) ve gerek ulusal gerekse uluslararası ölçekte yetkili makamlar arasında işbirliği,
2. Ulusal düzeyde olsun, AB düzeyinde olsun, karmaşık ve farklı yasal kurallar ve gelenekler ve kimi zaman bunlarla bir araya gelen zayıf uygulama,
3. Kanıtlar ve elektronik veriler meselesi,
4. Zaman. Mali soruşturmalar sıklıkla uzun zaman almakta ve zaman, insan gücü ve mali araçlar bakımından büyük miktarda kaynağa mal olmaktadır.

Rapor, aynı zamanda, herhangi bir yargı yetkisi alanı için geçerli olabilecek, Üye Devletler ve AB'ye yönelik bir dizi tavsiye içermektedir:

- Mali soruşturma; tek başına ekonomik ve mali suçların ötesinde, (terörizm içeren) tüm ciddi ve organize suç örneklerinde yürütülmelidir. Dolayısıyla, mali suçlar alanında karmaşık ve uzun soruşturmaları hızlandırmayı amaçlayan, savcılık da dâhil olmak üzere, ilgili tüm makamları içeren, kapsayıcı bir mali suçlar ve mali soruşturmalar politikası hazırlanmalıdır. AB düzeyinde üzerinde anlaşılmış olan ilgili

⁷¹Ayrıca bkz.: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/financial-investigation/index_en.htm

⁷²AB GENVAL 2012 karşılıklı değerlendirme beşinci raundu nihai raporu – "Mali Suçlar ve Mali Soruşturmalar". Ulaşmak için bkz.: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>

öncelikleri yansıtmalı ve proaktif soruşturmalar için temel oluşturmalarıdır. Özellikle AB seviyesinde, uluslararası işbirliğinden elde edilecek olası yararlar daha fazla dikkat edilmelidir.

- Mali suçlar ve mali soruşturmalar politikası uzun vadeli bir ulusal stratejiye yansımalarıdır. Mümkün olan her durumda, analiz ürünleri temelinde proaktif kolluk önlemleri alınabilmesi için mali istihbaratın öncülük ettiği bir polisiye yaklaşım stratejiye dâhil edilmelidir. Strateji, dâhil olan kuruluşlara yönelik sağlam bir raporlama mekanizması kadar, düzenli inceleme ve değerlendirme metodolojisi ile de birleştirilmelidir. Böyle bir strateji kurulurken hem seçilmiş yetkilere haiz farklı makamlar arasındaki görev tahsisini hem de ciddi uluslararası suç davalarını içeren kilit öncelikleri açıklığa kavuşturmak için bazı temel kriterler, kurallar veya kılavuzlar düşünülmelidir. Strateji, dolayısıyla, proaktif, istihbaratın öncülük ettiği bir yaklaşımı teşvik etmek adına, polis içerisinde sağlam bir yönetimle desteklenmelidir.
- Üye Devletler, cezai konularda karşılıklı tanıma ve adli işbirliği ile ilgili tüm AB mevzuatını uygulamalıdır. Dahası, Üye Devletler ve ilgili AB organları, ilgili Çerçeve Kararları'nın uygulanmasını ve hukuki yardımlaşma mekanizmalarının uygulanışı konusunda bir inceleme yapılmasını üstlenmelidir. Üye Devletler, bu yolla, yabancı kolluk makamları, AB organları ve diğer ilgili aktörler ile verimli bir proaktif veri alışverişi önündeki engelleri saptamalı ve bunların üstesinden gelmelidir. Suç kaynaklı gelirlerin ya da suç ile alakalı diğer mülklerin izlenmesi ve saptanması alanında Üye Devletler'in varlık geri kazanımı daireleri arasındaki işbirliği konulu, 6 Aralık 2007 tarihli ve 2007/845/JHA sayılı Konsey Kararı doğrultusunda gerçekleştirilen anlık bilgi alışverişleri daha da genişletilmeli ve Üye Devletler ile AB'nin kolluk makamları arasındaki bilgi ve istihbarat alışverişinin basitleştirilmesi konulu, 18 Aralık 2006 tarihli ve 2006/960/JHA sayılı Konsey Çerçeve Kararı teşvik edilmelidir.

4.2.1.2 PC-OC Anketi

Avrupa Konseyi'nin Cezai Meselelerde İşbirliğine Dair Avrupa Sözleşmelerinin İşleyişinden Sorumlu Uzmanlar Komitesi (PC-OC) 2014 yılında dikkatini suç gelirlerinin hedef alınması alanına odaklanmıştır. PC-OC Anketi'ne⁷³ verilen yanıtlar başka şeylerin yanı sıra, uluslararası işbirliği ile ilgili, Strazburg ve Varşova sözleşmeleri hükümlerinin uygulanışı konusunda Taraflar arasında farklılıklar olduğunu göstermiştir.

Ankette ele alınan konulardan bazıları şunlardır:

- Devletler, değer temelli olarak adlandırılan müsadere sistemlerine yaslanan taleplerin uygulamaya dökülmesini her zaman temin edememektedir. Bu sistem her iki sözleşmede de nesne temelli olarak adlandırılan müsadere sisteminin yanı sıra işbirliği yapılması olası bir sistem olarak tanımlanmaktadır. Her iki sistemde de bir ceza hükmü gereklidir. Değer temelli müsadere sisteminde, suç kaynaklı karlar hesaplanmaktadır. Nihayetinde hâkim, bu hesaplamalara dayanarak, elde edilen suç kaynaklı karlara eşdeğer bir para miktarının ödenmesini zorunlu kılmaktadır. Bundan sonra müsadere emri, hüküm giyen kişiye ait tüm varlıkları kapsayacak şekilde icra edilebilmektedir. Bu bakımdan, söz konusu varlıkların doğrudan doğruya ceza gerektiren suçtan elde edilmiş olduğunu kanıtlamaya gerek yoktur.

⁷³Müsadere edilen malların yönetimi ve varlık paylaşımı da dahil olmak üzere suç gelirlerinin zapt edilmesi ve müsadere alanındaki uluslararası işbirliği bakımından Avrupa Konseyi araçlarının kullanımı ve verimliliği anketi, PC-OC Mod (2015) 06Rev4, 19.5.2016. Ulaşmak için bkz.:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>

- Birçok Devlet *fili* olarak suçlanan/hüküm giyen kişiye ait olan ancak yasal olarak üçüncü bir kişiye, çoğu durumda paravan bir kişiye ait kabul edilen varlıkların zapt edilmesi ve müsadere olasılığını tanımaktadır.
- Sadece bazı Devletler, hükme dayanmayan müsadere ve diğer önlemler amacıyla veya bakımından hukuki yardımlaşma sağlama pozisyonundadır. Bu; suça ilişkin bilgilerin çoğu zaman suç gelirlerinin hükme dayanmayan şekilde kovuşturulması, aranması ve zapt edilmesi çerçevesinde kullanılmak üzere talep edildiği, bilgi toplama aşamasını içermektedir.
- Bazı Devletler suç gelirlerinin zapt edilmesi ve müsadere amacıyla tüzel kişilerin mali sorumlulukları ile ilgili cezai, umumi ve idari kovuşturmalarda yardım sağlama pozisyonundadır.
- Sadece bazı Devletler, özellikle zapt etme ve müsadere konularında Bitcoin gibi sanal para birimleri ile alakalı işlemlerde yardım sağlama pozisyonundadır.

4.2.1.3 MONEYVAL

Kara Para Aklama Karşıtı Önlemler ve Terörizmin Finanse Edilmesi Değerlendirmesinden Sorumlu Uzmanlar Komitesi – MONEYVAL,⁷⁴ Avrupa Konseyi'nin, kara para aklama ve terör finansmanına karşı koymaya yönelik başlıca uluslararası standartlara uygunluğu ve bunların uygulanışının etkililiğini ölçmek ve aynı zamanda sistemlerine yönelik gerekli iyileştirmeler konusunda ulusal makamlara önerilerde bulunmak görevi verilmiş olan bir daimi izleme organıdır.

MONEYVAL, dinamik bir karşılıklı değerlendirmeler süreci, akran denetimi ve raporların düzenli olarak takip edilmesi yoluyla, ulusal makamların kara para aklama ve terörizmin finanse edilmesi başlıklarında daha etkin mücadele etmeleri için kapasitelerini iyileştirme amacını gütmektedir.

Değerlendirme raporları internet üzerinde yayınlanmaktadır.⁷⁵

4.2.2 Siber Suç Hakkında Değerlendirme

4.2.2.1 GENVAL

AB karşılıklı değerlendirmeler yedinci raundu, siber suçların önlenmesi ve siber suçlarla mücadele alanındaki Avrupa politikalarının pratik uygulanışı ve işleyişine adanmıştır. Nihai olarak ortaya çıkan değerlendirme raporları kamuya açılmıştır ve diğer ülkelere siber suçlarla ilgili mevzuat ve stratejilerini gözden geçirmekte yardımcı olabilir.⁷⁶

Aynı zamanda, taslak nihai rapor, uluslararası işbirliği ile ilgili bazı sorunlu başlıkların altını çizmektedir; şöyle ki bir hukuki yardımlaşma talebine yanıt verilen ortalama süre birkaç ayı bulmakta ve hukuki yardımlaşmanın bir uluslararası anlaşma temelinde mi yoksa karşılıklılık temelinde mi sağlandığına bağlı olarak değişebilmektedir. İkinci durumda, yanıt verme süresi daha da uzamaktadır. Ancak, siber suçların özgünlüğü düşünüldüğünde, "Hukuki yardımlaşma işlemlerinin uzunluğu, soruşturma yürütülmesi ve başarısı açısından olumsuz sonuçlar doğuran hukuki yardımlaşma resmi kanallarını görece etkisiz kılmaktadır, zira dijital kanıtlar uçucudur, hızla ve verimli biçimde ele alınmaları gerekmektedir, çünkü gecikmeler verilerin kaybolmasına yol açabilmektedir. Dolayısıyla, siber suç soruşturmalarında hukuki yardımlaşma taleplerinin ele alınışını hızlandırmaya dönük genel

⁷⁴ Kara Para Aklama Karşıtı Önlemler ve Terörizmin Finanse Edilmesi Değerlendirmesinden Sorumlu Uzmanlar Komitesi (MONEYVAL): http://www.coe.int/t/dghl/monitoring/moneyval/default_en.asp?expandable=0

⁷⁵ Bkz.: <http://www.coe.int/en/web/moneyval/jurisdictions>

⁷⁶ Benimsenen raporlara şuradan ulaşabilirsiniz: <http://www.coe.int/da/web/octopus/blog/-/blogs/genval-evaluation-reports-on-cybercrime>

bir ihtiyaç vardır". Ayrıca taslak rapor; üçüncü Devletleri kapsayan hukuki yardımlaşma prosedürlerini iyileştirecek uluslararası çözümlerin bulunması gerektiğini not etmektedir; örneğin, verili bir devlette, hızlandırılmış veri çıkarma emri talepleri için icra makamlarının uzlaştığı bir formun kullanılması bir Üye Devlet'te belirlenen en iyi uygulama olarak belirtilmiştir. Benzer şekilde, bir hukuki yardımlaşma talebi göndermeden önce üçüncü Devletlerin yetkili makamları ile gayri resmi ve kişisel temaslar geliştirilmesi, bu türden resmi taleplerin yerine getirilmesi sırasında daha iyi ve daha hızlı işbirliği yapılabilmesine olanak sağlayabilecek, yararlı bir pratik olarak vurgulanmıştır.⁷⁷

Üye Devletlerin önüne aşağıdaki tavsiyeler konulmuştur:

- Üye Devletler başka ülkelere gönderdikleri hukuki yardımlaşma taleplerinin kalitesini iyileştirmelidir, özel olarak yeterli düzeyde tamamlanmış olmaları temin edilmeli ve hukuki yardımlaşma taleplerine verilen yanıtları hızlandıracak ve bunların kalitesini artıracak yöntemler incelenmelidir.
- Hukuki yardımlaşma kayıt sistemi ve kayıttan talepte bulunan devlete yanıt gönderilmesine kadar olan süre boyunca bir davanın izlenmesine imkân tanıyacak hukuki yardımlaşma yönetim sistemi oluşturmak yoluyla, Üye Devletlerin, diğer Üye Devletler ve üçüncü devletler ile olan iletişim süreçlerinin etkililiğini güçlendirmesi tavsiye edilmektedir.
- Üye Devletler Eurojust, EJM ve Europol araçlarını daha sık kullanmaya ve üçüncü devletlerden hukuki yardımlaşma taleplerine daha hızlı yanıt almak için yetkili yabancı makamlar ile gayri resmi temaslar kurmaya teşvik edilmektedir.
- AB, Üye Devletlerinden AB ülkesi olmayanlara giden hukuki yardımlaşma taleplerinin iletilmesi ve yerine getirilmesi açısından etkin bir yöntem oluşturmaya dönük çabaları koordine etmeyi veya ilgili AB dışı İSS'ler ile doğrudan işbirliği oluşturmaya yönelik bir çerçeve oluşturmayı düşünmelidir.
- AB, özellikle operasyonel bilgilerdeki alışveriş ve hukuki yardımlaşma talepleri ile bunların yerine getirilmesi bakımından, Üye Devletler ve başta Birleşik Devletler olmak üzere üçüncü devletler arasındaki iletişim sürecini iyileştirecek ve hızlandıracak çözümler üzerinde çalışmalıdır.

4.2.2.2 Siber Suçlar Komitesi

Avrupa Konseyi Siber Suçlar Sözleşmesi Komitesi; Budapeşte Siber Suçlar Sözleşmesi'nin uygulanışını izlemekte ve daha ileri standartlar ve kılavuz notlar çıkarmaktadır; bunların amacı hukuk, politika ve teknoloji alanındaki gelişmeler ışığında, Budapeşte Sözleşmesi'nin etkin şekilde kullanılmasını ve uygulanmasını kolaylaştırmaktır.

4.2.2.2.1 Hukuki yardımlaşma

Hukuki yardımlaşma; ceza kovuşturmalarında kullanılmak üzere yabancı yargı yetkisi alanlarından kanıtların alınmasında başlıca araç olmaya devam etmektedir. Aralık 2014'te Siber Suçlar Komitesi, Budapeşte Sözleşmesi hukuki yardımlaşma hükümlerinin işleyişine ilişkin değerlendirmeyi tamamlamıştır.⁷⁸ Başka şeyler yanında, hukuki yardımlaşma sürecinin hem genel olarak hem de özel olarak elektronik kanıtları elde etme bakımından verimsiz kabul edildiği sonucuna ulaşmıştır. Taleplere yanıt sürelerinin altı ila 24 ay arasında olması norm gibi görünmektedir. Pek çok talepten ve dolayısıyla soruşturmadan

⁷⁷"Siber suçların önlenmesi ve siber suçlarla mücadele konusundaki Avrupa politikalarının pratik uygulanışı ve işleyişi" hakkında karşılıklı değerlendirmeler yedinci raundu taslak nihai raporu", Haziran 2017. Bkz. s. 82-88. Ulaşmak için bkz.: <http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>

⁷⁸T-CY(2013)17rev, 3 Aralık 2014, Siber Suçlar Komitesi değerlendirme raporu: Budapeşte Siber Suçlar Sözleşmesi hukuki yardımlaşma hükümleri. Ulaşmak için bkz.: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>

vazgeçilmiştir. Bu da hükümetlerin toplumu ve bireyleri siber suçlara ve elektronik kanıtların işin içine girdiği diğer suçlara karşı koruma pozitif yükümlülüğünü olumsuz etkilemektedir.

Değerlendirme Raporu, ayrıca, tüm veri türlerinin aynı sıklıkla veya aciliyetle gerekmediği sonucuna varmıştır: talep edilen veri türleri bakımından, abone bilgileri en sık istenen bilgi olarak diğerlerinden ayrılmaktadır. Bu türden bilgilere yönelik büyük talep miktarları, hukuki yardımlaşma taleplerini işleme almaktan ve yerine getirmekten sorumlu makamların üzerinde ağır bir yük oluşturmakta ve ceza soruşturmalarını yavaşlatmaktadır (ve sık sık engellemektedir). Bu da abone bilgilerine ilişkin güçlüklerle getirilecek çözümlerin hukuki yardımlaşmayı daha verimli hale getireceğini düşündürmektedir.

Siber Suçlar Sözleşmesi Komitesi raporu aşağıdaki sorunlarla karşılaşıldığını saptamaktadır:

- Hukuki yardımlaşma taleplerini hazırlamak veya hukuki yardımlaşma taleplerini yerine getirmek için gerekli olan prosedürlerin süresi, iş yükü ve karmaşıklığı
- Genel olarak veya belirli ülkelerle alakalı olarak taleplere verilen yanıtlardaki gecikmeler (6 – 24 ay)
- Abone verilerini sağlamadaki gecikmeler
- Bazı ülkelerin “küçük” suçlar konusunda işbirliği yapmayı reddetmesi
- Bazı ülkelerin işbirliği yapmayı reddetmesi veya yanıt vermemesi
- 7/24 iletişim noktaları ile işbirliğindeki sorunlar
- Hukuki yardımlaşma talebinin alındığına veya verilerin muhafaza edilmiş olduğuna dair belge verilmemesi
- “Acil” taleplere yönelik açık olmayan kriterler
- Kullanılan dil, çeviri kalitesi, terminoloji sorunu
- Büyük miktarda veriye yönelik olarak çok geniş açıyla gelen talepler
- Hukuki sistemler arasındaki açılar; örneğin soruşturma yetkileri ile alakalı açılar
- Yasal sınırlamalar (verilerin korunması)
- Hukuki yardımlaşma talebi olmaksızın yabancı devletin işbirliğini reddetmesi. Ancak, hukuki yardımlaşma yabancı Devlet’in işbirliği olmaksızın elde edilemeyecek, yeterli bilgi ve kanıtları gerektirebilmektedir (kısır döngü)
- Talep, talepte bulunulan Devlet’in yasal eşliğini veya resmi şartlarını karşılamayabilmektedir ya da talep tamamlanmış olmayabilmekte veya eşik/gereken standart çok yüksek olabilmektedir
- Kanunların yetersizliği
- Bir eylemin her iki ülkede de suç sayılması şartının gerçekleşmemesi
- Hukuki yardımlaşma talebinden önce verilerin mevcut olmaya devam etmesini güvence altına alacak muhafaza talebinin yapılmamış olması
- Muhafaza talebine rağmen yabancı Devlet’te verilerin muhafaza edilmemesi
- Yabancı devlette veya kendi devletinizde verilerin artık mevcut olmaması
- Sağlayıcıların verileri erişilebilir kılmaya yönelik farklı politikaları olması
- Yabancı Devlet içerisinde fevkalade hallerde iletişim kurulacak kişinin veya yetkili makamın bilinmiyor olması, ilgili yetkililerin, örneğin internet barındırma hizmeti sağlayıcılarının saptanması güç olabilmektedir
- Çok fazla talep nedeniyle aşırı yüklenme
- Elektronik kanıtlar konusunda talepte bulunulan Devlet’teki teknik bilgiler ve anlayışın sınırlı oluşu
- Adli kolluğun sınırlı yetkileri olması
- “Olası neden” eşığı.

Siber Suçlar Sözleşmesi Komitesi; siber suç ve elektronik kanıtlar ile ilgili olarak, Budapeşte Siber Suçlar Sözleşmesi ve diğer anlaşmaların mevcut hükümlerinin daha etkin kullanımı üzerinden hukuki yardımlaşma sürecini daha verimli kılacak bir dizi tavsiye benimsemiştir, ama aynı zamanda tavsiyelerini önerdiği ek çözümlere dayandırmıştır⁷⁹. Bunlar örneğin şunları içermektedir:

- Taraflar; Budapeşte Sözleşmesi muhafaza yetkilerini eksiksiz şekilde uygulamalıdır (Tavsiye 1), hukuki yardımlaşma sürecinin etkililiğini izlemelidir (Tavsiye 2), hukuki yardımlaşma alanına daha fazla ve daha iyi eğitilmiş personel tahsis etmelidir (Tavsiye 3 ve 4), 7/24 iletişim noktalarının rol ve kapasitelerini kuvvetlendirmelidir (Tavsiye 5), fevkalade haller için prosedürler oluşturmalıdır (Tavsiye 8) vs.
- Taraflar (muhtemelen Budapeşte Sözleşmesi'ne getirilecek bir Protokol yoluyla) abone bilgilerinin hızlandırılmış ifşasına (Tavsiye 19), uluslararası bilgi çıkarma emirleri olasılığına (Tavsiye 20), adli makamlar arasında dolaysız işbirliğine (Tavsiye 21), yabancı hizmet sağlayıcılarından dolaysız şekilde bilgi elde etme pratiğinin ele alınmasına (Tavsiye 22), Taraflar arasında ortak soruşturmalar ve/veya ortak soruşturma ekipleri kurulmasına (Tavsiye 23), taleplerin İngilizce dilinde gönderilmesine (Tavsiye 24) izin vermeyi gözden geçirmelidir.

4.2.2.2.2 Ek pratik güçlükler

Uluslararası işbirliği ile de ilgili olan bazı ek güçlükler ve başlıklar ayrıca detaylandırılacaktır:

Veriler yurtdışında depolanıyor olsa bile, açık olan şüpheli bilgisayarından içerik verilerine erişme koşulları, bağlantılı rıza ve yargı yetkisi alanı sorusu

Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu tarafından hazırlanan, buluttaki elektronik kanıtlara ceza yargılaması erişimi ile ilgili nihai rapor: Siber Suçlar Sözleşmesi Komitesi dikkatine sunulan tavsiyeler⁸⁰ konusunda çalışan, Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu'nun (BKG) nihai raporunda, bir kural olarak kolluk yetkilerinin ülkelerin egemenlik alanları ilkesiyle belirlendiği belirtilmiştir. Bu ilke çerçevesinde, hiçbir devlet kendi yargı yetkisini bir başka egemen devletin egemenlik alanında tatbik edemez. Başka yargı yetkisi alanlarında bulunan sunuculardaki veya genel olarak bilgisayar sistemlerindeki verilere, söz konusu yargı yetkisi alanlarındaki makamların dahil olmaksızın, ceza yargılaması erişimi yapılması endişe konusudur.

Ancak, bir suç mahallindeki veya oluşturulmakta olan bir kişiye ait bir bilgisayarın "açık" (yani çalışmakta ve aktif) olduğu durumlarda, ceza yargılaması makamları, teknik olarak, sunucunun yer aldığı ve verilerin saklandığı yargı yetkisi alanının bilgisi olmaksızın, (bulut sunucularında saklananlar da dâhil olmak üzere) verilere erişebilmektedir. Budapeşte Sözleşmesi'nin 32b Maddesi, Aralık 2014'te Siber Suçlar Sözleşmesi Komitesi tarafından benimsenen Kılavuz Not'ta tanımlanan ancak çok sınırlı durumlara bir çözüm önermektedir.⁸¹

⁷⁹ Bkz. Siber Suçlar Sözleşmesi Komitesi değerlendirme raporu s. 125-127: Budapeşte Siber Suç Sözleşmesi hukuki yardımlaşma hükümleri.

⁸⁰ T-CY (2016)5, 16 Eylül 2016, Buluttaki elektronik kanıtlara ceza yargılaması erişimi: Siber Suçlar Sözleşmesi Komitesi dikkatine sunulan tavsiyeler. Ulaşmak için bkz.:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

⁸¹ Siber Suçlar Sözleşmesi Komitesi Sınırlar arası Erişim hakkında Kılavuz Not # 3 (Madde 32), 3 Aralık 2014, Ulaşmak için bkz.: <https://rm.coe.int/16802e726a>

Budapeşte Sözleşmesi Madde 32b'nin sınırlılıkları nedeniyle ("açık" sistemleri konu alan soruşturmalar sırasında e-posta erişimine şüphelinin gönüllü rızası), bazı devletler pratikte tek taraflı çözümler aramaktadır. Belirli bir ceza soruşturmasında kolluk kuvvetlerinin farklı, bilinen bir ülkeye bağlandıklarını bilseler dahi, eğer cihaz açıksa ya da erişim bilgileri kanuni yollardan elde edilmişse, yalnızca şüphelinin cihazındaki verilere değil, ama aynı zamanda e-posta veya diğer bulut hizmeti hesapları türünden bağlantılı araçlardaki verilere de erişimleri yaygın bir pratik gibi görünmektedir.

BKG; sınır aşan AB anti tröst yasası doktrinini araştırmış (Davalar *ICI* 48/69; *Woodpulp* 89/85) ve Avrupa Komisyonu'nun Avrupa Birliği içerisindeki rekabet kurumlarının anti tröst kovuşturmalarda kanıt toplamak üzere dünya genelindeki sunuculara erişim sağlayabilmesini tavsiye ettiğini kaydetmiştir. Kurumların elektronik kanıtları toplamak konusunda etkin yetkilere sahip olmaları için inceleme yetkilerinin uygulanışında, mülkü incelenmekte olan kuruluş veya kişi için erişilebilir olan dijital bilgileri, bu bilgilerin, ilgili ulusal rekabet kurumunun toprakları dışındaki veya Avrupa Birliği dışındaki sunucular veya diğer depolama araçları da dahil olmak üzere nerede depolandığından bağımsız olarak, toplayabilmeleri önem taşımaktadır. Verilere bu türlü erişimin koşulları ve emniyet tedbirleri bir protokolde tanımlanmalıdır.

BKG; bir sınırlar arası erişim çerçevesinin, bireylerin haklarının korunması ve diğer hükümetlerin veya tebaalarının yetkileri veya haklarına hanel gelmesinin engellenmesi için, verilere bu türden erişim konusunda şartları ve emniyet tedbirlerini tanımlaması gerekeceği sonucuna varmıştır.

Abone verilerine erişim

Abone verileri mahremiyet bakımından daha az hassasiyet içermekte olup en sık talep edilenlerdir. Pek çok devlette polis veya savcı emri yeterli olmaktadır, ancak bazı devletler dinamik İP söz konusu olduğunda, kimi akış verileri de gündeme geldiği için, mahkeme emri talep etmektedir.

Dolayısıyla, buluttaki elektronik kanıtlara ceza yargılaması erişimi konulu nihai raporunda BKG şu tavsiyelerde bulunmuştur:

- Abone bilgileri, akış verilerine ve içerik verilerine göre mahremiyet bakımından daha az hassas olduğuna göre, abone bilgilerinin çıkarılmasına yönelik emirlerde şartlar, diğer veri türleri veya diğer müdahaleci yetki türlerinde olduğundan daha hafif emniyet tedbirlerine tabi olmalıdır.
- Abone bilgilerinin çıkarılmasında uygulanacak daha hafif bir rejim, bulut bağlamında yürütülen yurtiçi soruşturmaları ve uluslararası işbirliğini kolaylaştıracaktır.

Bir devletin egemenlik alanı içerisinde hizmet sunan çok uluslu bir hizmet sağlayıcısının söz konusu olduğu bir örnekte, hizmet sağlayıcısının yurtdışındaki merkezinden ve verilerin bulunduğu yerden bağımsız olarak, abone verilerinin çıkarılmasını içeren yurtiçi emrinin koşulları (Budapeşte Sözleşmesi Madde 18) araştırılmıştır.

Bir ceza yargılaması makamı, bilgisayar sisteminin veya depolama cihazının yerine (Budapeşte Sözleşmesi Madde 19 arama ve zapt etme hükümleri bu konuyu kapsamaktadır) ya da aranan verileri elinde tutan veya kontrol eden (hizmet sağlayıcıları

da dahil olmak üzere) gerçek veya tüzel kişinin yerine odaklanarak kolluk yetkisi tespiti yapabilmektedir.⁸² İkincisi çıkarma emirleri ile ilgili 18. Madde kapsamındadır.

Hukuki yardımlaşma aranan verilerin yerinin bilindiğini, dolayısıyla bir yardımlaşma talebinin hangi Devlet'e ve hangi yetkili makama iletileceğinin bilindiğini ve talebin gerçekleştirilebilir olduğunu varsaymaktadır. Ancak, verilerin hangi yargı yetkisi alanında depolandığı ve/veya verilere hangi yasal rejimin uygulandığı, ceza yargılaması makamları için çoğu zaman açık değildir. Bir hizmet sağlayıcısının merkezi, bir yargı yetkisi alanında iken, ikinci bir yargı yetkisi alanının yasal rejimi geçerli olabilmekte ve bu arada veriler üçüncü bir yargı yetkisi alanında depolanıyor olabilmektedir. Veriler birden fazla yargı yetkisi alanına yansıyıp bunlar arasında hareket edebilmektedir. Eğer verilerin yeri yargı yetkisi alanını belirliyor ise, bir bulut hizmet sağlayıcısının ceza yargılaması erişimini önleyecek biçimde sistematik olarak verilerin yerini değiştirmesi akla gelebilmektedir.

İnternetin bu açıdan sınırları olmadığı için, bir soruşturmada ihtiyaç duyulan abone bilgileri bir Taraf'ın "egemenlik alanında hizmet sunan" bir hizmet sağlayıcısının elinde olabilmekte, fakat sağlayıcı fiilen başka bir yargı yetkisi alanında olup aranan bilgiler bir diğer yargılama yetkisi alanındaki sunucularda depolanıyor olabilmektedir.

BKG; Budapeşte Sözleşmesi'nin 18.1.b sayılı maddesinin mantıklı bir yorumunun bir çözüm sunduğu görüşündedir. Bir Taraf'ın yetkili makamları, bilgilerin nerede saklandığından ve sağlayıcının nerede yerleşik olduğundan bağımsız olarak, kendi egemenlik alanı üzerinde hizmet sunan bir hizmet sağlayıcısından abone bilgilerini talep edebiliyor olmalıdır. Siber Suçlar Sözleşmesi Komitesi tarafından benimsenen, abone bilgileri çıkarma emirlerini konu alan Kılavuz Not # 10⁸³ Budapeşte Sözleşmesi Madde 18'in bu şekilde yorumlanmasını ve uygulanmasını teşvik etmektedir. Bu uygulama hukuki yardımlaşma talebinden etkin biçimde kaçınılmaktadır.

Kılavuz Not; Madde 18.1.b kapsamında emirlerin, eğer hizmet sağlayıcısı abone bilgilerini elinde tutuyorsa veya kontrol ediyorsa ve eğer hizmet sağlayıcısı "Tarağ'ın egemenlik alanında hizmet sunuyorsa," belirtilen abonelere yönelik olarak belirli durumlarda uygulanabileceğini vurgulamaktadır." Bu belirli durumlar şunlardır:

- Hizmet sağlayıcısının Taraf'ın egemenlik alanındaki kişilerin hizmetlerine abone olmasına izin verdiği (ve örneğın bu türden hizmetlere erişimi engellemediğı) durumlar;
- Hizmet sağlayıcısının faaliyetlerini bu türden abonelere yönlendirdiğı (örneğin, yerelde reklam verdiği veya Taraf ülkenin dilinde reklam yaptığı) veya faaliyetleri sırasında abone bilgilerini (veya bağlantılı akış verilerini) kullandığı veya Taraf'taki abonelerle etkileşime girdiğı durumlarda;
- Çıkarılacak abone bilgilerinin bir sağlayıcının Taraf'ın egemenlik alanında sunulan hizmetleri ile ilişkili olduğu durumlar.

Ayrıca Belçika Yüksek Mahkemesi kararı da bir devletin egemenlik alanında faaliyet gösteren hizmet sağlayıcısının uygulanabilir ulusal mevzuatın konusu olduğu ve söz konusu mevzuatla bağlandığı hükmüne vararak bu yorumu teyit etmiştir. Yahoo! davasında⁸⁴

⁸² Bkz. örneğın 6 Temmuz 2016 tarihli, ağ ve bilgi sistemlerinin güvenliğı konulu, 2016/1148 sayılı Avrupa Birliğı Direktifi ("NIS Direktifi"), Madde 18 Yargı yetkisi alanı ve egemenlik alanı.

⁸³ Kılavuz Not #10: 28 Şubat 2017'de Siber Suçlar Sözleşmesi Komitesi tarafından çıkarılan yazılı prosedür ile benimsenen abone bilgileri çıkarma emirleri (Budapeşte Sözleşmesi Madde 18). Ulaşmak için bkz.: <https://rm.coe.int/doc/09000016806f943e>

⁸⁴1 Aralık 2015'te Yahoo! davasında hükme varan Belçika Yüksek Mahkemesi, şu nihai karara varmıştır: ABD, California'da kayıtlı bulunan Yahoo! Inc. abone bilgilerini çıkarmaya mecburdur ve dolayısıyla Belçika Ceza Muhakemeleri Usulü Kuralları Madde 46 paragraf (§)2 uyarınca alınacak zorlayıcı tedbirlere tabidir .

Ulaşmak için bkz. (Felemenkçe): http://iure.iuridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1

Belçika Yüksek Mahkemesi, bir Taraf'ın egemenlik alanında hizmet sunan ve dolayısıyla "bulunan" bir sağlayıcıya yönelik bir abone bilgileri çıkarma emrinin (Madde 18.1.b'de geçtiği haliyle) yurtiçi nitelikli bir emir olduğunu ve uluslararası işbirliği konusu ya da yargılama yetkisinin egemenlik alanı dışına taşan uygulanışı olmadığını hükme bağlamıştır. Yahoo! Inc. daha önceki, 20 Kasım 2013 tarihli Antwerp Temyiz Mahkemesi kararına karşı temyize gitmiş bulunmaktaydı; diğer nedenlerin yanı sıra uluslararası teamül hukuku çerçevesinde, bir Devletin egemenlik alanı dışında yargılama yetkisini uygulayamayacağı gerekçesini ileri sürmüştü.

Belçika Yüksek Mahkemesi şunları hükme bağlamıştır:

- Genel olarak bir Devlet ancak kendi egemenlik alanında zorlayıcı tedbirler uygulayabilir, aksi halde bir başka Devlet'in egemenliğini ihlal etmiş olur.
- "Bir Devlet'in kendi egemenlik alanında zorlayıcı tedbirler dayatması için söz konusu önlemler söz konusu bölge arasında yeterli bir mekânsal bağlantı olması gerekmektedir."
- Belçika Ceza Muhakemeleri Usulü Kuralları Madde 46, paragraf (§)2'ye kadar; "Belçika'da faal olan operatör ve tedarikçilere, sadece, soruşturma süreci Belçika kovuşturma makamlarının yetkisi dahilinde olan suçlar söz konusu olduğunda ancak kimlik verileri elde etmek amacıyla tedbir uygulamayı amaçlamaktadır. Bu tedbir Belçika Polisi veya Sulh Yargıçlarının ya da kendi adlarına hareket eden ajanların yurtdışındaki varlığını gerektirmemektedir. Bu tedbir yurtdışında herhangi bir maddi eylem de gerektirmemektedir. Dolayısıyla bu önlemin sınırlı bir kapsamı ve dayanağı vardır, uygulanışı Belçika egemenlik alanı dışında herhangi bir müdahale gerektirmemektedir".
- Yahoo! Inc., "ücretsiz bir ağ postası hizmeti tedarikçisi olarak, Belçika egemenlik alanında varlık göstermekte ve özel olarak "www.yahoo.be" alan adını kullanarak, yerel dil kullanımıyla, hizmetlerinin tanıtımını kullanıcılarının mekanı temelinde yaparak ve bu kullanıcılar için bir şikayet kutusu ve Sıkça Sorulan Sorular Masası kurarak Belçika'da erişilebilir olmasıyla Belçika iktisadi yaşamına aktif olarak katılarak kendisini Belçika hukukuna gönüllü olarak tabi kılmaktadır."
- "Savcı; Birleşik Devletler'deki herhangi bir Amerikan vatandaşından herhangi bir şey talep etmemektedir, fakat Belçika topraklarında hizmet sunan bir Amerikan vatandaşından Belçika'da bir şey talep etmektedir".
- Dolayısıyla egemenlik alanı dışında yargılama yetkisi kullanımı söz konusu değildir.

Çok uluslu hizmet sağlayıcıları ile doğrudan işbirliği

ABD ile işbirliği özellikle önem taşımaktadır, zira çok uluslu hizmet sağlayıcılarının birçoğunun merkezi oradadır ve hukuki yardımlaşma taleplerinin sayısı artmaktadır. Buluttaki elektronik kanıtlara ceza yargılaması erişimi ile ilgili BKG nihai raporu, Birleşik Devletler hizmet sağlayıcılarının, yasal talebe istinaden abone bilgileri ve akış verilerini ifşa edebileceği ve bunun Budapeşte Sözleşmesi'nin Madde 18.1.b ile uyum içinde olduğunu vurgulamaktadır. Ancak, sağlayıcı politikalarının uçuculuğu⁸⁵ ve ifşanın öngörülemez oluşu, hem müşteriler hem de kolluk kuvvetleri açısından öngörülemez bir durum yaratmakta ve hukukun üstünlüğü ile ilgili meseleleri gündeme getirmektedir.

⁸⁵ Çeşitli sağlayıcıların politikalarına ilişkin bir genel özet için bkz. Buluttaki verilere ceza yargılaması erişimi: "yabancı" hizmet sağlayıcıları ile işbirliği, Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu, Mayıs 2016. Ulaşmak için bkz.: <https://rm.coe.int/168064b77d>

Avrupalı sağlayıcılar söz konusu olduğunda bu türden işbirliği veri koruma kuralları nedeniyle mümkün olmamaktadır ve hukuki yardımlaşma talebi sunulması gerekmektedir.

ABD’li hizmet sağlayıcıları, yabancı makamlardan dolaysız olarak alınan her türlü veri muhafaza talebini, bu talebi hukuki yardımlaşma yoluyla ifşa talebinin izleyeceği beklentisiyle kabul etmektedirler. Avrupalı sağlayıcılar başka yargı yetkisi alanlarındaki kolluk makamlarından dolaysız şekilde gelen muhafaza taleplerini kabul etmemektedir.

Fevkalade hal prosedürleri

Siber Suçlar Sözleşmesi Komitesi yasal yardımlaşma konulu Değerlendirme Raporu Tavsiye 8, Tarafların, yaşam riskleri ve benzeri fevkalade haller ile ilişkili taleplere yönelik olarak fevkalade hal prosedürleri oluşturmaya teşvik edildiklerini belirtmektedir. 2016 yılında BKG tarafından gerçekleştirilen ve 33 Devlet’in katıldığı bir anket çalışması⁸⁶ göstermektedir ki:

- Tarafların büyük bölümünün yürürlükte fevkalade hallerde yurtdışındaki ceza yargılaması makamlarına verilerin ifşa edilmesine izin veren bir mevzuatı bulunmamaktadır;
- % 20’sinden azının yürürlükte yurtdışındaki yetkili makamlarının yabancı makamlara hızlandırılmış bir biçimde veri ifşa etmesine izin veren prosedürleri bulunmamaktadır;
- Yalnızca iki Taraf fevkalade hallerde egemenlik alanları üzerindeki hizmet sağlayıcılarının yabancı yetkili makamlara veri ifşa etmesine izin vermektedir.

BKG, Tavsiye 8’in Budapeşte Sözleşmesi’ne eklenecek bir Protokol yoluyla ele alınmasını da önermiştir.

Budapeşte Sözleşmesi’ne Ek Protokol

BKG; daha etkin bir hukuki yardımlaşmaya olanak yaratılması, ihtiyaç halinde ve şartlarla emniyet tedbirlerine tabi şekilde, diğer yargı yetkisi alanlarındaki hizmet sağlayıcıları ile dolaysız işbirliğinin kolaylaştırılması, verilere sınırlar arası erişim konusunda mevcut pratikler ile ilgili olarak şartlarla emniyet tedbirlerinin çerçevelendirilmesi ve oluşturulması ve veri koruma gerekliliklerinin oluşturulması için Budapeşte Siber Suçlar Sözleşmesi’ne getirilecek ek bir protokolün müzakeresine başlanmasını tavsiye etmiştir.

Budapeşte Sözleşmesi’ne getirilecek bir protokol:

- Diğer yargı yetkisi alanlarındaki hizmet sağlayıcıları ile dolaysız işbirliğine yönelik prosedürleri, şartları ve ceza kovuşturmalarında alınan verilerin kabul edilebilirliğini açıklığa kavuşturabilir;
- Yabancı hizmet sağlayıcılarına yapılacak dolaysız muhafaza talepleri için bir yasal temel oluşturabilir. Bu hâlihazırda ABD’deki hizmet sağlayıcıları tarafından kabul edilen bir uygulamadır;
- Belirli fevkalade hallerde yabancı yargı yetkisi alanlarındaki hizmet sağlayıcıları ile dolaysız şekilde işbirliğine gidilmesine izin veren fevkalade hal prosedürlerini öngörebilir.

⁸⁶ Hukuki yardımlaşma kanalları üzerinden veya hizmet sağlayıcılarına yapılan dolaysız talepler üzerinden bir başka yargı yetkisi alanında saklanan verilerin derhal ifşa edilmesi için yapılan fevkalade hal talepleri, Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu, Mayıs 2016

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>

Bir Protokol'ün olası unsurları:

- Daha etkin hukuki yardımlaşma hükümleri:
 - abone bilgilerine yönelik olarak hukuki yardımlaşma taleplerinde basitleştirilmiş bir rejim;
 - uluslararası veri çıkarma emirleri;
 - hukuki yardımlaşma taleplerinde adli makamlar arasında dolaysız işbirliği;
 - ortak soruşturmalar ve ortak soruşturma ekipleri;
 - İngilizce dilinde talepler;
 - tanıkların, mağdurların ve uzmanların işitsel/görsel olarak dinlenmesi;
 - Fevkalade hal hukuki yardımlaşma talepleri.
- Abone bilgileri, muhafaza talepleri ve fevkalade hal talepleri ile ilgili olarak diğer yargı yetkisi alanlarındaki hizmet sağlayıcıları ile dolaysız işbirliğine izin veren hükümler.
- Verilere sınırlar arası erişim konusundaki mevcut uygulamalarda daha açık bir çerçeve ve daha güçlü emniyet tedbirleri.
- Veri koruma gereklilikleri de dâhil olmak üzere emniyet tedbirleri.

Budapeşte Siber Suçlar Sözleşmesi 2. Ek Protokol taslağının hazırlanmasına yönelik Görev Tanımı, Haziran 2017'de Siber Suçlar Sözleşmesi Komitesi'nin 17. Genel Oturumunda benimsenmiştir.⁸⁷

4.3 Hukuki Yardımlaşmaya Yönelik Şablon ve Formların Kullanımı

Hukuki yardımlaşma talepleri, uluslararası yasal araçlara dayansalar dahi çeşitlilik sergilemektedirler, zira hem alıcı Devlet'in mevzuat kaynaklı ve pratik beklentilerine hem de gönderen Devlet'in ulusal mevzuatına bağımlıdır. Hukuki yardımlaşma talebi formları bir dereceye kadar Devletlere yardımcı olabilmektedir; bu nedenle model şablonların geliştirilmesi için bazı çabalarda bulunulmuştur.

Avrupa Konseyi Komitesi PC-OC 2016'da cezai konularda yardımlaşmaya yönelik bir model talep formu geliştirmiştir⁸⁸.

Siber Suçlar Sözleşmesi Komitesi, Budapeşte Siber Suçlar Sözleşmesi hukuki yardımlaşma hükümleri ile ilgili 2014 Değerlendirme Raporu Tavsiye 17'de, Avrupa Konseyi'nin (kapasite geliştirme projeleri çerçevesinde) Madde 31 taleplerine yönelik olarak çok dilli standartlaştırılmış şablonlar geliştirmesi veya bu tip şablonlara bağlanması gerektiğini belirtmiştir⁸⁹.

⁸⁷ T-CY(2017)3 Budapeşte Siber Suçlar Sözleşmesi 2. Ek Protokol taslağının hazırlanmasına yönelik Görev Tanımı, Haziran 2017. Ulaşmak için bkz.: <https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-protocol/168072362b>

⁸⁸ 69. Toplantı belgeleri (Mayıs 2016) için bkz.: Hukuki yardımlaşma model talep formu taslağı ve uygulayıcılar için uygulama kılavuzları: <http://www.coe.int/en/web/transnational-criminal-justice-pcoc/pc-oc-69th-meeting>
<http://www.coe.int/en/web/transnational-criminal-justice-pcoc/model-request-form-for-mutual-assistance-in-criminal-matters>

⁸⁹ Budapeşte Siber Suçlar Sözleşmesi hukuki yardımlaşma hükümleri, 3.12.2014 (T-CY(2013)17rev).
(<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>)

Siber uzayda ceza yargılamasının iyileştirilmesi hakkında AB Konseyi sonuçları (Haziran 2016), başka şeyler yanında, Komisyon'a, Üye Devletler, Eurojust ve üçüncü ülkeler ile bağlantılı olarak, e-kanıtların güvence altına alınması ve elde edilmesi talebinde bulunmak üzere kullanılan mevcut standartlaştırılmış form ve prosedürlerin, uygun hallerde, nasıl benimseneceğine ilişkin düşünüp tavsiyelerde bulunmaları çağrısında bulunmuştur.

Bir müsadere emri formu örneği, müsadere emirlerinin karşılıklı olarak tanınması ilkesinin uygulanması ile ilgili, 6 Ekim 2006 tarihli, 2006/783/JHA sayılı Konsey Çerçeve kararında bulunabilir⁹⁰.

Bir başka örnek; cezai konularda Avrupa Soruşturma Emri ile ilgili 3 Nisan 2014 tarihli, 2014/41/EU sayılı Avrupa Parlamentosu ve Konsey Direktifi'dir⁹¹.

Son olarak, Birleşmiş Milletler Uyuşturucu ve Suç Ofisi, bir Hukuki Yardımlaşma Talebi Yazım Aracı geliştirmiştir⁹².

Geleneksel hukuki yardımlaşma yaklaşımlarının internet suçlarının olduğu küresel bir dünyada artık yeterli olmadığı açıktır. Avrupa Konseyi'nin her iki aracı, Budapeşte Sözleşmesi (örneğin buluttaki verilere erişim) ve Varşova Sözleşmesi (dondurma ve müsadere emirlerinin uygulanması) çerçevesinde de, olanakların ve güçlüklerin bilincine varılması, siber suç soruşturmalarını ve paralel mali soruşturmaları birleştirirken, daha iyi sonuçlar alınmasına katkıda bulunacaktır.

⁹⁰<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006F0783&from=EN>

⁹¹<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>

⁹²<https://www.unodc.org/mla/en/index.html>

5 Sanal Para Birimleri

Kripto para birimleri, özellikle de Bitcoin, suç oluşturan hizmetlere ödeme yapılmasında olsun, haraç mağdurlarından ödeme almakta olsun, siber suçların çoğunda tercih edilen para birimi olmaya devam etmektedir. Böyle olmasına rağmen, Bitcoin topluluğunun alım-satımla uğraşanlar türünden kilit üyeleri, kendilerini, giderek artan bir şekilde siber suçluların mağduru oldukları durumlar içinde bulmaktadır⁹³. Temel eğitimde verilen sanal para birimlerine giriş dersinden devam eden ileri eğitim, sanal para birimlerinin (özel olarak da Bitcoin'in) işleyişi konusunda daha detaylı bilgiler ve bu sanal para birimlerinin kullanımı ile bağlantılı risklere ilişkin bir tartışma sunmaktadır. Bu bölüm; sanal para birimleriyle ilişkili olarak deneyimlenmiş olan, soruşturma ve dondurma/zapt etme güçlüklerini tanıtarak son bulmaktadır.

5.1 Temel Eğitim Tekrarı

MEGG tanımları⁹⁴ temelinde, temel eğitim sanal para birimleri ile alakalı olarak aşağıdaki terim ve kategorileri tanımlamıştır:

- Sanal para birimi
- Elektronik para/e-para
- Dijital para birimi
- Dönüştürülebilir sanal para birimi, dönüştürülemeyen sanal para birimi
- Merkezi sanal para birimi, âdemi merkezi sanal para birimi

Bu terimler aşağıdaki tabloda tekrar özetlenmektedir.

Sanal Para Birimi	"Sanal para, internet üzerinden alım satımı yapılabilen bir dijital değer ifadesi olup ve (1) bir değişim aracı ve/veya (2) bir hesap birimi ve/veya (3) bir değer deposu olarak işlev görmektedir; ancak herhangi bir yargı yetkisi alanında yasal ödeme aracı statüsüne sahip değildir"
Elektronik para / e-para	"Sanal para birimi, itibari para birimi cinsinden gösterilen değer elektronik olarak transfer edilmesinde kullanılan itibari para biriminin dijital temsili olan e-paradan da farklıdır."
Dijital para birimi	"Dijital para birimi, sanal para biriminin (itibari olmayan) veya e-paranın (itibari) dijital gösterimi anlamına gelebilmekte ve bu nedenle sıklıkla sanal para birimi terimi ile eşanlamlıymış gibi kullanılmaktadır."
Dönüştürülebilir sanal para birimi, dönüştürülemeyen sanal para birimi	Dönüştürülebilir (veya açık) sanal para birimi, gerçek para biriminde eşdeğer bir değere sahiptir ve gerçek para birimi ile iki yönlü olarak daima takas edilebilmektedir. Dönüştürülemeyen (veya kapalı) sanal para biriminin belirli bir sanal alana veya dünyaya özgü olması amaçlanmıştır ve kullanımını düzenleyen kurallar uyarınca itibari para birimi ile takas edilememektedir.

⁹³Organize İnternet Suçları Tehdidi Değerlendirmesi (IOCTA) 2016, Europol. Ulaşmak için bkz.:

<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>

⁹⁴ MEGG Raporu, Sanal Para Birimleri Kilit Tanımlamaları ve Kara Para Aklama Karşıtı Önlemler ve Terörizmin Finanse Edilmesi ile Mücadele Açısından Ortaya Çıkan Potansiyel Riskler, Haziran 2014. Ulaşmak için bkz.:

<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

Merkezi sanal para birimi, âdemi merkezi sanal para birimi	Merkezi sanal para birimlerinin tek bir yönetici otoritesi (yöneticisi); yani sistemi kontrol eden üçüncü bir tarafı olmaktadır. Bir yönetici para birimini çıkarır, kullanımının kurallarını belirler, merkezi bir ödeme defteri tutar ve para birimini tekrar satın alma (dolaşımdan geri çekme) yetkisine sahiptir. Merkezi olmayan sanal para birimleri ise herhangi bir merkezi yönetim otoritesi ve merkezi izleme ya da gözetimi olmayan, dağıtık, açık kaynaklı ve matematik tabanlı eşler arası sanal para birimleridir.
---	---

5.2 Sanal Para Birimlerine Giriş

5.2.1 Daha Fazla Sanal para Birimi Terminolojisi⁹⁵

Kripto para	Kriptografi ile korunan, matematik tabanlı âdemi-merkezi bir sanal para birimine atıfta bulunmaktadır; yani dağıtılmış, âdemi-merkezi ve güvenli bir bilgi ekonomisini uygulamak için kriptografi ilkelerini içermektedir. Kripto para birimi, bir kişiden (şahıs veya kuruluş) diğerine değer aktarması yapmak için kamu ve özel anahtarlara yaslanmaktadır ve her transfer edildiğinde kriptografik olarak imzalanmalıdır. Kripto para birimi defterlerinin güvenliği, bütünlüğü ve dengesi, rastgele dağıtılmış bir ücret (Bitcoin’de, az sayıda yeni üretilen, "blok ödülü" adını taşıyan Bitcoin ve ayrıca bazı örneklerde kullanıcılar tarafından bir sonraki bloğa kendi işlemlerini dâhil etmeleri için madencilere bir teşvik olarak ödenen işlem ücretleri) alma şansı karşılığında ağı koruyan, (Bitcoin’de, madenciler olarak anılan) karşılıklı olarak güvensiz taraflar ağı tarafından temin edilmektedir. İşlemleri doğrulamak ve blok zincirini korumak için bir çalışma kanıtı sistemi kullanan, çoğunlukla Bitcoin’den türetilen, yüzlerce kripto para birimi şartnamesi tanımlanmıştır. Bitcoin, eksiksiz şekilde uygulanan ilk kripto para birimi protokolünü sağlamış olsa da, hisse kanıtlarına dayalı sistemler gibi alternatif, potansiyel olarak daha verimli kanıtlama yöntemlerinin geliştirilmesine ilgi artmaktadır.
Bitcoin	2009 yılında başlatılan ilk ademi-merkezi, dönüştürülebilir sanal para birimi ve ilk kripto para birimiydi. Bitcoin’ler, para biriminin birimlerini oluşturan ve yalnızca kullanıcılar onlar için ödeme yapmak istediğinde değer taşıyan benzersiz sayı ve harf dizilerinden oluşan hesap birimleridir. Bitcoin’ler, yüksek derecede anonimlik içeren kullanıcılar arasında dijital olarak işlem görmekte ve ABD Doları, Avro ve diğer itibari veya sanal para birimlerine dönüştürülebilmektedir (satın alınabilir veya nakde dönüştürülebilir).
Etherum	Tam bir programlama dili içeren tek kripto para birimi (onun çatalı Ethereum Classic hariç). Akıllı sözleşmeler; önceden belirlenmiş koşullar yerine getirildikten sonra bir ödemenin gönderildiği kendi kendine çalışan komut dizileri oluşturmak için kullanılabilir.

⁹⁵MEGG Raporu, Sanal Para Birimleri Kilit Tanımlamaları ve Kara Para Aklama Karşıtı Önlemler ve Terörizmin Finanse Edilmesi ile Mücadele Açısından Ortaya Çıkan Potansiyel Riskler, Haziran 2014. Ulaşmak için bkz.: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

Altcoin	Bitcoin dışındaki matematik tabanlı, âdemi merkezi, dönüştürülebilir sanal para birimine, bu türden para birimlerinin ilkinde atıfta bulunmaktadır. Örnekler arasında Ripple, PeerCoin, Lite-Coin, zerocoin, anoncoin ve dogecoin bulunmaktadır.
Monero	Nisan 2014'te oluşturulan, hem gönderme hem de alma adresleri perdelendiğinden geleneksel izlemeyi etkisiz kılan çeşitli teknolojileri kullanarak muhtemelen en yüksek mahremiyet düzeyini sağlayan, açık kaynaklı bir kripto para birimidir. İşlem tutarı gizlidir. İşlemlerin gizlilik özellikleri varsayılan olarak sağlanmaktadır.
Düğüm	İşlemleri Bitcoin ağı üzerinden diğer düğümlere yayan bir istemci.
Özel anahtar	Gizli anahtar, Bitcoin işlemlerini yürütmeye izin vermekte ve işlemler için sahtesi yapılamayacak bir imza oluşturmak için kullanılmaktadır. Özel anahtarın sahibi, Bitcoin'leri kontrol etmektedir.
Genel anahtar	Özel anahtardan türetilmiş herkesçe bilinen anahtar.
Bitcoin işlemi	Bitcoin'ler bir adresten diğerine taşınmaktadır. Bir işlem yaparken, kullanıcı, bilgisayarına kurulmuş bir Bitcoin cüzdanı veya ilgili işlevleri sunan bir çevrimiçi hizmet kullanmaktadır. Bitcoin işlemi, geri alınamayan, bir kerelik bir işlemdir. Bitcoin işlemleri şeffaftır ve internette çeşitli şekillerde görüntülenebilmektedirler. Gönderenin Bitcoin adresi, alıcının Bitcoin adresi ve işlemde yer alan Bitcoin miktarı gibi veriler görüntülenebilmektedir.
Zapt Etme	Bitcoin'lerin bir şüpheli adresinden kolluk kuvvetleri tarafından kontrol edilen bir adrese taşınması.
Gizleyici (gizleyen araç)	Bir Bitcoin işleminin kaynağını gizlemek ve anonimliği kolaylaştırmak için tasarlanmış araçlara ve hizmetlere atıfta bulunmaktadır.
Mikser (çamaşır hizmeti, tambur)	Bu, tüm işlemleri aynı Bitcoin adresinde birbirine bağlayarak ve onları başka bir adresten gönderilmiş gibi gösterecek şekilde beraberce göndererek blok zincirindeki işlem zincirini gizleyen bir anonimleştirici türüne verilen addır. Bir mikser veya tambur, işlemleri, belirli sanal sikkeleri (adresleri) belirli bir işlemle bağlantılandırmayı son derece zorlaştıran karmaşık, yarı rastgele, aptalca bir işlemler dizisi üzerinden göndermektedir. Mikser hizmetleri, bir kullanıcıdan belirli bir Bitcoin adresine para gönderme talimatları olarak çalışmaktadır. Mikser hizmeti daha sonra bu işlemi diğer kullanıcı işlemleriyle "karıştırmakta", öyle ki kullanıcının fonları kime yönlendirmeyi istediği belirsiz hale gelmektedir.
Tor (Soğan Yönlendirici)	İnternette, yeraltında, dağıtılmış bir bilgisayar ağına verilen addır. Bu ağ dünyanın her yerinden çok sayıda bilgisayar aracılığıyla iletişimi yönlendirerek ve bunları çok sayıda şifreleme katmanına sararak gerçek IP adresini ve dolayısıyla ağın kullanıcılarının kimliklerini gizlemektedir.
Karanlık Cüzdan	Şu özellikleri bir araya getirerek Bitcoin işlemlerinin anonimliğini temin etmeyi amaçlayan tarayıcı tabanlı bir uzantı cüzdanına verilen isimdir: otomatik anonimleştirici (mikser), ademi merkezi ticaret, sansürlü kalabalık fonlama platformları, hisse senedi platformları, bilgi karaborsaları ve İpek Yolu'na benzer ademi merkezi pazar yerleri.
Soğuk Depolama	Çevrimdışı bir Bitcoin cüzdanına; yani internete bağlı olmayan bir Bitcoin cüzdanına atıfta bulunmaktadır. Soğuk depolama,

	depolanan sanal para biriminin hekleme ve hırsızlığa karşı korunmasına yardımcı olmayı amaçlamaktadır.
Sıcak Depolama	Soğuk Depolama'ya kıyasla, çevrimiçi bir Bitcoin cüzdanına atıfta bulunmaktadır.
Yerel Takas Ticaret Sistemi (YTTS)	Üyelerin gruptaki diğer kişilerle mal ve hizmet alışverişinde bulunmalarını sağlayan, yerel olarak örgütlenmiş bir ekonomik kuruluştur. YTTS, mal ve hizmet karşılığında işlem yapılabilen veya takas edilebilecek değer birimlerini temsil etmek için yerel olarak oluşturulmuş bir para birimi kullanmaktadır. Teorik olarak Bitcoin'ler bir YTTS ile kullanılan yerel para birimi olarak kabul edilebilir.

5.2.2 Sanal Para Birimi Katılımcıları

Takasçı (sanal para birimi takası olarak da bilinir)	Bir ücret (komisyon) karşılığında gerçek para birimi, fonlar ya da diğer sanal para birimleri ve aynı zamanda değerli metaller karşılığında sanal para takasını ve bu işlemlerin tersini bir iş olarak yapan kişi ya da kuruluştur. Takasçılar genellikle nakit, banka havaleleri, kredi kartları ve diğer sanal para birimleri dâhil olmak üzere geniş bir ödemeler yelpazesini kabul etmekte ve yönetici bağlantılı, bağlı olmayan veya üçüncü taraf sağlayıcısı olabilmektedirler. Takasçılar, borsa veya döviz masası olarak hareket edebilmektedirler. Bireyler tipik olarak sanal para birimi hesaplarına para yatırmak ve sanal para birimi hesaplarından para çekmek için takasçıları kullanmaktadır.
Yönetici	Merkezi bir sanal para birimi ihraç etme (dolaşıma sokma), kullanımı için kurallar belirleme, merkezi ödeme defteri tutulması işleriyle uğraşan ve sanal para birimini tekrar satın alma (dolaşımdan çekilme) yetkisine sahip olan kişi veya kuruluştur.
Kullanıcı	Sanal para elde eden ve bunu gerçek veya sanal mal veya hizmetleri satın almak veya kişisel yetkisiyle başka bir kişiye (kişisel kullanım için) havaleler göndermek için kullanan veya sanal parayı (kişisel) bir yatırım olarak elinde tutan kişi veya kuruluştur.
Madenci	Sanal para birimi sistemindeki işlemleri doğrulamak için kullanılan, dağıtılmış bir çalışma kanıtı veya başka bir dağıtılmış kanıt sistemi üzerinden karmaşık algoritmaları çözmek üzere özel bir yazılım çalıştırarak âdemi merkezi bir sanal para birimi ağına katılan kişi veya kuruluş. Madenciler, kendi kendilerine yalnızca kendi amaçları için dönüştürülebilir sanal para birimi oluşturuyorlarsa kullanıcı olabilirler. Madenciler, sanal para birimini itibari para birimleri veya diğer sanal para birimleri karşılığında satmak üzere bir iş olarak sanal para birimi üreterek sanal bir para birimi sistemine takasçı olarak da katılabilirler.
Sana para birimi cüzdanı (müşteri) Cüzdan sağlayıcısı	Bitcoin'leri veya diğer sanal paraları elde tutmak, depolamak ve aktarmak için bir araçtır (yazılım uygulaması veya başka bir şey). Bitcoin'leri veya diğer sanal paraları elde tutmak, saklamak ve aktarmak için sanal para cüzdanı sağlayan bir kuruluştur. Cüzdan, kullanıcının blok zincirdeki sanal para birimi adresine tahsis edilmiş sanal parayı kullanmasına izin veren özel anahtarlarını taşır. Cüzdan sağlayıcısı, kullanıcıların, takasçıların ve tüccarların

sanal para birimi işlemlerini daha kolay yürütmesine izin vererek bir sanal para birimi sistemine katılmayı kolaylaştırır. Cüzdan sağlayıcısı, müşterinin sanal para birimi bakiyesini tutar ve ayrıca genellikle depolama ve işlem güvenliği sağlar.

Diğer çeşitli kuruluşlar da bir sanal para birimi sistemine katılabilmekte ve takasçılar ve/veya yöneticilere bağlı ya da onlardan bağımsız olabilmektedir. Bunlar, diğerleri arasında, ağ yönetim hizmeti sağlayıcılarını (yani ağ yöneticilerini), (tüccar kabulünü kolaylaştıran) üçüncü taraf ödeme işlemcilerini, yazılım geliştiricilerini ve uygulama sağlayıcılarını içermektedir.

5.2.3 Bitcoin

Bitcoin, merkezi bir otorite veya aracı olmayan, kullanıcılar tarafından desteklenen, âdemi merkezi ve eşler arası bir ödeme ağıdır. Satoshi Nakamoto 2009⁹⁶ yılında ilk Bitcoin şartnamesini ve konsept kanıtını bir kriptografi posta listesine yayınlamıştır. Temel olarak, Bitcoin ağının amacı ve çalışması, “blok zincir” olarak bilinen herkese açık bir defterin yönetimi ve paylaşımı ile ilgilidir. Bu defter, yapılan tüm işlemleri içermekte ve her işlemin geçerliliğini doğrulamak için kullanılmaktadır⁹⁷. Defterdeki işlemlerin bütünlüğü ve kronolojik sıralaması, kriptografi ile gerçekleştirilmektedir. Bitcoin, genellikle bir kripto para birimi olarak da bilinen dönüştürülebilir, âdemi merkezi bir sanal para birimidir.

Bu bölüm bitcoin sanal para biriminin nasıl işlediğine dair bir açıklama sunmaktadır.

5.2.3.1 Değer Aktarımı

Bir sanal para birimi ile ilgili en bariz soru; para birimi kullanıcılarının birbirlerine nasıl değer aktardıkları sorusudur. Bitcoin örneğinde, her bir kullanıcının bir ya da daha fazla Bitcoin adresi vardır. Kullanıcılar istedikleri kadar Bitcoin adresi yaratabilmekte, hatta isterlerse her bir işlem için ayrı bir adres yaratabilmektedirler. Pratikte, Bitcoin yazılımı ve hizmetleri bir kullanıcının Bitcoin’lerini bir “cüzdan”da saklanıyormuş gibi gösterir. Bir cüzdan söz konusu yazılım veya hizmetin özelliklerine bağlı olarak, tek bir Bitcoin adresini veya çok sayıda adresi temsil edebilmektedir. Adres, belirli bir Bitcoin sahipliğini temsil etmek üzere kullanılan eşsiz bir tanımlayıcı değer olarak işlev görmektedir⁹⁸. A kişinin B kişisine para gönderebilmesi için, Bitcoin ağına, gönderici adresi kimlik numarasını, alıcı adresi kimlik numarasını (alıcı adresi) ve Bitcoin transfer miktarını içeren bir mesaj gönderirler. Bu mesajı alan, Bitcoin ağındaki her bir düğüm defter kopyalarını güncelleyecek ve ardından işlem mesajını diğer düğümlere iletacaktır.

Bir saldırgan olan C kişinin, Bitcoin’leri A kişinin cüzdanından kendi cüzdanına aktarmaya çalışan bir mesajı yayınlamasını önlemek için, işlemlerin gerçekliği A kişinin dijital imzasının varlığı sayesinde güvence altına alınmaktadır. A kişinin cüzdanından Bitcoin’leri aktaran geçerli bir işlem mesajı yaratmak için, mesajı üreten kişi cüzdanın özel anahtarı ile ilişkilendirilmiş şifreye sahip olmalıdır.

5.2.3.2 Sahipliğin Kanıtlanması

Yukarıdaki örnekte, alıcı olan B kişisi, alınan Bitcoin’lerin gerçekte A kişisine ait olduğunu nasıl bilebilir? Bitcoin’lerin göndericisinin Bitcoin’leri aktarmak için geçerli bir mesaj üretmesi için söz konusu Bitcoin’lerin mevcut sahibi olduğunu kanıtlaması gerekmektedir.

⁹⁶ <https://bitcoin.org/en/faq>

⁹⁷ <https://bitcoin.org/en/how-it-works>

⁹⁸Kesin olarak, her adres bir kamusal / özel anahtar çiftidir. Kamusal anahtar “adres”tir. Özel anahtar gizli tutulur ve adresi içeren işlemleri dijital olarak imzalamak ve böylece işlemin gerçekliğini doğrulamak için kullanılır.

A kişinin B kişisine beş Bitcoin gönderdiğini varsayalım. A kişisi, kendisinin işlemin alıcısı olduğu ve daha önceki işlemlerin toplam değerinin beş Bitcoin'den fazla olduğu önceki işlemlere ait referansı işleme dâhil etmek zorundadır. Bunlara işlemin "girdi"leri denmektedir.

Bitcoin ağının tüm kullanıcıları, önceki tüm işlemlerin geçmişini içeren defterin ("blok zinciri") bir kopyasını muhafaza etmektedir. Ardından, B kişisi, A kişinin işlemine yapılan girdilerde atıfta bulunulan Bitcoin'lerin, A kişisine ait olduğunu doğrulayabilir. Bu işlemi basitleştirmek için, işlemlerin birbirini tutması kuralı vardır. Diğer bir deyişle, bir işlemde "girdiler" içindeki Bitcoin sayısı, işlemin "çıktıları" içindeki Bitcoin sayısına eşit olmalıdır. Bir eşitsizlik varsa, A kişisi girdilerin kalan bakiyesini kendilerine aktarabilmektedir.

5.2.3.3 Çifte Harcama

Bitcoin ağı gibi eşler arası bir ağda, işlemlerin ağdaki herhangi bir düğüm tarafından alınma sırasının, oluşturuldukları sırayla aynı olası garantisi yoktur. Pratik açıdan bu, A kişinin B kişisine Bitcoin gönderen bir işlem mesajı oluşturmasını ve daha sonra aynı anda Bitcoin'leri başka birine göndermek için ikinci bir işlem mesajı oluşturmasını mümkün kılar. Bu çift harcama olarak bilinmektedir. Bitcoin ağındaki bazı düğümlerin ilk önce ikinci işlemi alması tamamen olasıdır. Bir süre sonra ilk işlem bu düğümlere ulaştığında, geçersiz sayılır çünkü hâlihazırda kullanılmış olan girdileri, onların perspektifinden, başka bir işlemde tekrar kullanılmaktadır. Bitcoin protokolünün temsil ettiği temel teknolojik ilerleme, bu sorunun çözüldüğü mekanizmadır.

İşlemler bloklar olarak bilinen gruplar halinde birleştirilmekte ve bloklar bir blok zinciri oluşturmak üzere birbirine bağlanmaktadır. Bir blok içerisindeki işlemlerin aynı anda gerçekleştiği kabul edilmektedir. Bloklar, her bloğun zincirdeki önceki bloğa atıfta bulunması sayesinde sıralanmaktadır. Hâlihazırda blokta olmayan işlemlere "onaylanmamış" adı verilmektedir. Ağdaki herhangi bir düğüm, bir dizi onaylanmamış işlemi toplayabilir, bunları bir blok içerisine yerleştirebilir ve bunları zincirdeki bir sonraki blok olarak önerebilir. Önerilen blok, hesaplanması zor karmaşık bir matematik problemine çözüm getirmelidir⁹⁹. Bitcoin ağı, matematik probleminin zorluğunu, yeni bir bloğun blok zincirine her on dakikada bir ekleneceği şekilde dinamik olarak ayarlamaktadır¹⁰⁰.

Pek olası olmamakla birlikte, Bitcoin ağındaki birden fazla düğümün aynı anda bloklar önermesi durumu yaşanabilir. Bu durumda, blok zincir geçici olarak ağdaki farklı düğümler olarak ayrılır, blok zincirine farklı bloklar ekler. Bir sonraki blok zincire eklendiğinde durum çözülür. Daha önce de belirtildiği gibi, yeni blok, zincirdeki önceki bloğa bir referans içerecektir. Bu nedenle, blok zincirindeki iki olası daldan birine eklenecek ve bir dalı diğerinden daha uzun hale getirecektir. Bitcoin ağında düğümler bir kural olarak mevcut olan en uzun dala geçmelidir ve sonuç blok zincirinin çok hızlı bir şekilde dengelenmesidir. Ayrıca, tüm düğümler zincirin sonundan biraz geride kalan tüm bloklarda hemfikir olacaktır. Bu nedenle, Bitcoin aktarımına dayalı olarak mal gönderimi yapmadan evvel bir süre beklemenin daha güvenli olduğu düşünülmektedir. Her bir bloğun zincire eklenmesi yaklaşık olarak on dakika sürdüğü için, altı bloğun beklenmesi bir saat beklemek anlamına gelecektir.

5.2.3.4 Madencilik

⁹⁹Bloku oluşturan düğüm öyle bir sayısal değer bulmalıdır ki, bu değer bloğun diğer verisiyle birleştiğinde sonuç olarak elde edilen birleşik veriye belirli bir sınırın altında bir kriptografik karma değer vermelidir.

¹⁰⁰ Bu, karmaşık hesaptaki eşik değerinin düşürülmesiyle sağlanır, yani daha az sayıda kabul edilebilir cevap vardır ve böylece geçerli bir değer tanınması daha zor hale gelir.

Yukarıda anlatılan, blok inşa etme ve bunları blok zincirine ekleme süreci madencilik olarak bilinmektedir. Bloğu kim çözer ve onu blok zincirine eklerse, 25 Bitcoin ödül kazanmaktadır. Nihayetinde artık piyasaya Bitcoin sürülmeyene kadar her dört yılda bir blok ödülü yarıya indirilecektir. Toplam 21 milyon Bitcoin üretilecektir.

Bitcoin ödülüne ek olarak, madenciler işlemlere tercihe göre eklenebilecek olan bir işlem ücreti de alabilmektedirler. Şu anda madenciliğin başlıca ödülü blok ödülüdür fakat zaman içinde işlem ücretleri madenciliğin teşvik edicisi haline gelecektir.

Madenciliğin büyük bölümü bireyler tarafından değil, madencilik havuzları olarak bilinen madenci grupları tarafından yapılmaktadır. Blokları çözmenin ödülü, havuz üyeleri arasında, her bir üyenin havuza sağladığı blok çözme çabası miktarıyla orantılı olarak bölünmektedir.

5.3 Sanal Para Birimi Riskleri

Gerçek para ve diğer sanal para birimleri ile takas edilebilen dönüştürülebilir sanal para birimleri pek çok nedenle kara para aklama ve terörizm finansmanı istismarına potansiyel olarak açıktır. Bu bölüm; mali bütünlüğe dönük bu iki tehdidin her ikisi ile alakalı olarak sıralanan riskleri anlatacaktır¹⁰¹.

Birincisi, Geleneksel nakit dışı ödeme yöntemlerinden daha büyük bir anonimliğe izin verebilmektedirler. Sanal para sistemleri internet üzerinden işlem görebilir, genellikle yüz yüze olmayan müşteri ilişkileri niteliğine sahiptir ve anonim fonlamaya izin vermektedir (finansman kaynağını uygun bir şekilde tanımlamayan sanal takasçılar yoluyla nakit finansmanı veya üçüncü taraf finansmanı). Gönderen ve alıcı yeterince iyi şekilde tanımlanmamışsa, anonim transferlere de izin verebilirler. Âdemi merkezi sistemler anonimlik ile alakalı risklere karşı özellikle savunmasızdırlar. Örneğin, tasarımı gereği, hesaplar olarak işlev gören Bitcoin adresleri, isimler veya müşteri kimliğine ilişkin başka bilgi taşımaz ve sistemde merkezi bir sunucu veya hizmet sağlayıcısı yoktur. Bitcoin protokolü, katılımcıların tanımlanmasını ve doğrulanmasını gerektirmemekte veya öngörmemektedir ya da gerçek dünya kimliğiyle bağlantılandırılmak zorunda olan işlem geçmiş kayıtları oluşturmamaktadır.

Şüpheli işlem kalıplarını izlemek ve tanımlamak için şu anda herhangi bir merkezi gözetim organı ve kara para aklama karşıtı yazılım bulunmamaktadır. Kolluk kuvvetleri, soruşturma veya varlık zapt etme amaçlarıyla tek bir merkezi konumu veya kuruluşu (yönetici) hedef haline getirememektedir (ancak yetkililer, takasçının toplayabileceği müşteri bilgileri için tek tek takasçıları hedef alabilmektedir). Dolayısıyla, geleneksel kredi ve banka kartları veya PayPal gibi daha yerleşik çevrimiçi ödeme sistemleri ile mümkün olmayan bir anonimlik potansiyeli seviyesi taşımaktadırlar. Sanal para birimlerinin küresel erişimi de taşıdığı potansiyel kara para aklama / terör finansmanı riskini artırmaktadır.

Sanal para birimi sistemlerine (cep telefonları da dâhil olmak üzere) internet üzerinden erişilebilmekte ve bunlar sınır ötesi ödemeler ve kaynak aktarımları için kullanılabilir. Ek olarak, sanal para birimleri, genellikle, kaynak aktarmak ve ödemeleri gerçekleştirmek için çoğunlukla birden fazla ülkeye yayılmış olan, birden fazla kuruluş içeren karmaşık altyapılara yaslanmaktadır. Hizmetlerin bu şekilde bölünmesi; kara para aklama / terör finansmanı konusundaki uygunluk ve denetim / icra sorumluluklarının açık olmayabileceği anlamına gelmektedir. Dahası, müşteri ve işlem

¹⁰¹Sanal para birimlerinin finansal sisteme ilişkin olarak ortaya çıkardığı riskleri sıralayan Avrupa Bankacılık Otoritesi tarafından mükemmel bir doküman hazırlanmıştır. Ulaşmak için bakın:

<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

kayıtları, çoğu zaman farklı yargı yetkisi alanlarında bulunan farklı kuruluşlar tarafından muhafaza edilebilir ki bu da kolluk kuvvetleri ile düzenleyici kurumların söz konusu kayıtlara ulaşmasını zorlaştırmaktadır. Sanal para teknolojisi ve iş modellerinin hızla gelişen niteliği, örneğin sanal para birimi ödeme sistemlerinde hizmet sağlayan katılımcıların sayısının tür ve rollerinin değişmesi sorununu şiddetlendirmektedir. Önemli bir nokta şu ki bir sanal para birimi sisteminin bileşenleri, yeterli kara para aklama / terör finansmanı kontrolleri olmayan yargı yetkisi alanlarında yerleşik olabilmektedir. Merkezileşmiş sanal para sistemleri kara para aklama suçlarına katılmış olabilir ve bilerek zayıf kara para aklama / terör finansmanı rejimlerine sahip yargı yetkisi alanları arayabilirler. Anonim kişiler arası işlemlere izin veren, âdemi merkezi dönüştürülebilir sanal para birimleri herhangi bir ülkenin erişiminin tümüyle dışında olan bir dijital evrende var olmakta gibi görünebilir.

Sanal para birimlerine ilişkin MEGG risk değerlendirmesi¹⁰² en azından yakın vadede yalnızca itibari para birimleri ve düzenlemeye tabi tutulan mali sistem ile değer takası yapabilen dönüştürülebilir sanal para birimlerinin kara para aklama / terör finansmanı riskleri oluşturmasının olası olduğunu belirtmektedir. Buna göre, atıfta bulunulan raporda tanımlanan risk temelli yaklaşım çerçevesinde, ülkeler kara para aklama / terör finansmanı ile ilgili çabalarını riski daha yüksek olan dönüştürülebilir sanal para birimlerine odaklamalıdır.

Risk değerlendirmesi, aynı zamanda, kara para aklama / terör finansmanı kontrollerinin, dönüştürülebilir finansal para birimi düğümlerini (yani, düzenlemeye tabi finansal sisteme geçiş sağlayan kesişme noktaları) hedeflemesi gerektiğini ve mal veya hizmet satın almak için sanal para elde eden kullanıcıları düzenlemeye tabi kılmayı amaçlamaması gerektiğini ileri sürmektedir. Bu düğümler, diğerlerinin yanı sıra, üçüncü taraflar olarak dönüştürülebilir sanal para birimi takasçılarına da içermektedir. Bu örneklerde, MEGG Tavsiyeleri çerçevesinde düzenlenmeye tabi tutulmalıdırlar¹⁰³. Dolayısıyla, ülkeler, uluslararası standartlarda belirtilen ilgili kara para aklama / terör finansmanı karşıtı gereklilikleri, dönüştürülebilir sanal para birimi takasçılarına ve dönüştürülebilir sanal para faaliyetlerinin düzenlemeye tabi itibari para mali sistemi ile kesiştiği düğümler olarak hareket eden diğer kurum tiplerine uygulamayı düşünmelidir.

MEGG'in risk temelli yaklaşımı çerçevesinde, ülkeler, sanal para gönderen, alan ve saklayan, fakat sanal paralar ile itibari paralar arasında takas veya nakit alım satımı hizmetlerini sunmayan mali kurumları veya diğer atanmış kuruluşları düzenlemeyi de düşünebilir.

Değiştirilen 5. Kara Para Aklama Karşıtı Direktif¹⁰⁴ sanal para birimi takas platformlarını ve cüzdan sağlayıcılarını, "yükümlü kuruluşları" tanımlayan Direktif tarafından yükümlülüğü getirilen kara para aklama düzenlemeleri sahasına çekecektir.

¹⁰²Sanal Para Birimleri – Risk Temelli bir Yaklaşım için Kılavuz, Mali Eylem Görev Gücü, Haziran 2015. Ulaşmak için bkz.: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

¹⁰³Şüpheye yer bırakmamak adına, MEGG Tavsiyeleri – Kara Para Aklama, Terörizmin Finanse Edilmesi ve Silahlanma ile Mücadelede Uluslararası Standartlar, Mali Eylem Görev Gücü, Şubat 2012. Ulaşmak için bkz.: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

¹⁰⁴http://www.consilium.europa.eu/register/en/content/out?typ=SET&i=ADV&RESULTSET=1&DOC_TITLE=&CONTENT_S=&DOC_ID=15849%2F17&DOS_INTERINST=&DOC_SUBJECT=&DOC_SUBTYPE=&DOC_DATE=&document_date_from_date=&document_date_from_date_submit=&document_date_to_date=&document_date_to_date_submit=&MEET_DATE=&meeting_date_from_date=&meeting_date_from_date_submit=&meeting_date_to_date=&meeting_date_to_date_submit=&DOC_LANGD=EN&ROWSPP=25&NRROWS=500&ORDERBY=DOC_DATE+DESC

ÜZERİNE DÜŞÜNÜLECEK SORULAR

1. Sanal paradan gerçek paraya dönüşüm nerede gerçekleşmektedir?
2. Bitcoin sanal para sisteminde bir işlemin tarafları nasıl tanımlanmaktadır?
3. Âdemi merkezi sanal para birimlerinin hangi temel özelliği onları düzenlemeyi zorlaştırmaktadır?
4. Bitcoin işlemlerinin herkese açık defterine ne ad verilmektedir?

5.4 Soruşturmadaki Güçlükler¹⁰⁵

5.4.1 Sanal Para Birimlerinin Kullanılmış Olduğunu Bilmek

Sanal para birimlerini içeren soruşturmalardaki ilk güçlük sanal para birimi kullanımını ve/veya suç kaynaklı varlıkların sanal para birimi biçiminde tutulup tutulmadığını tespit etmektir. Sanal para birimlerinde, değer ifadesi neredeyse her zaman elektronik biçimde muhafaza edilmektedir¹⁰⁶.

Bu nedenle, soruşturma görevlilerinin suç kaynaklarının sanal paraya çevrilmiş olma ihtimalinin bilincinde olması gerekmektedir. Adli dijital analizcilerin de zapt edilen elektronik depolama ortamlarında sanal para kullanımının nerede/nasıl aranacağını anlama kapasitesi ve becerisi olmalıdır.

5.4.2 İşlemlerin Anonimliği

Dağıtılmış sanal para birimlerinin başlangıcından beri, işleyişlerinin sıkça belirtilen bir özelliği, işlemlerin iddia edilen anonimliğidir. Bu nedenle, belki de Bitcoin'i içeren soruşturmalardaki başlıca güçlük, belirli bir Bitcoin cüzdanının faaliyetlerini gerçek dünyadaki bir bireyle ilişkilendirmektir.

Tüm Bitcoin işlemleri ve cüzdan içerikleri blok zincirinde herkes tarafında görülebilmekte ise de, özel kilide sahip değilseniz, bir başka hesap sahibine Bitcoin aktarımı yapamazsınız¹⁰⁷. Ancak, belirli bir özel kilide sahip olan gerçek dünyadan bir birey, Bitcoin aktarım işlemi üzerinden açığa çıkmamaktadır.

Belirli durumlarda, belirli işlemlerle ilişkilenen İP adreslerine yol veren teknikler tespit edilmiştir¹⁰⁸. Bu tekniklerin en eskilerinden biri, 2014 yılında Philip ve Diana Koshy tarafından yayınlanan bir akademik makalede tanımlanmıştır¹⁰⁹. Bitcoin ağındaki her bilgisayar tarafından iletilen her bir veri paketinin bir kopyasını indiren kendi Bitcoin yazılımı sürümlerini inşa etmişlerdir. Bu verilerin analizi sayesinde Koshys, belirli Bitcoin işlemlerinin arkasındaki İP adreslerinin tanımlanmasına izin veren belirli veri kalıplarını belirleyebilmişlerdir. Ancak, şimdilik, bu tür tekniklerin, içerdikleri hesaplama zorlukları nedeniyle ceza soruşturmalarının çoğunluğu açısından erişilebilir olmaları muhtemel değildir.

¹⁰⁵Aşağıdaki tartışmanın, merkezi olmayan sanal para birimi örneği olarak Bitcoin'e yer yer atıfta bulunduğu belirtilmeli. Burada açıklanan güçlükler, sanal para birimlerinin, özellikle âdemi merkezi sanal para birimlerinin büyük çoğunluğu için geçerlidir.

¹⁰⁶Sanal para birimi değerinin fiziksel ifadelerini satan bazı kuruluşlar vardır, ancak bunlar son derece nadirdir ve yaygın olarak kullanılmamaktadır. Örneğin, bkz. <http://www.coindesk.com/10-physical-bitcoins-good-bad-ugly/>

¹⁰⁷Bitcoin'lerin nasıl işlediğine ilişkin bir açıklama için bkz. yukarıdaki vaka çalışması.

¹⁰⁸<http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin>

¹⁰⁹P2P Ağ Akışı Kullanan Bitcoin'de Anaonimlik Analizi, Koshy ve diğ. http://fc14.ifca.ai/papers/fc14_submission_71.pdf

5.4.3 Kaynakların Kaynağı için Kimlik Saptama

Sanal para birimlerinin kullanıldığı saptandığı soruşturmalarda, bazı durumlarda, fonların yasadışı yollardan elde edilmiş olduğunun tespit edilmesi gerekebilmektedir. Şüpheli bu hususta sorgulanabilmekte fakat şüphelinin işbirliğine açık olmadığı ve/veya soruşturma altında olduklarını henüz anlamadığı örneklerde, sanal para birimlerinin nasıl satın alındığını tespit etmek güç olabilmektedir.

Bu bağlamda, özel sektörden gelecek yardım büyük önem taşımaktadır. Uygunluk gösteren kuruluşlar olan sanal para birimi takasçıları¹¹⁰ bireysel müşteriler hakkında bilgiler sağlayabilmektedir; tipik olarak isimleri, doğrulanmış iletişim detaylarını, İP günlük kayıtlarını, faaliyet kayıtlarını, takasta kullanıcı tarafından kullanılan tüm sanal para birimi adreslerini, kişisel mesajları, ödeme bilgilerini, kimlik ve ev adresi bilgilerini saklayacaklardır.

Budapeşte Sözleşmesi'nin siber suçlarla ilgili olarak öngördüğü usul yetkilerinin kullanımı da takasçılar ve sanal para birimleri ekosistemindeki diğer katılımcılar tarafından tutulmakta olan verilere erişime izin verecektir (örneğin muhafaza emirleri, akış verilerinin gerçek zamanlı olarak vs.)

Bir Bitcoin işleminde fon kaynağının tanımlanmasındaki güçlük bir mikser hizmetinin kullanımı ile daha da zorlaştırılmaktadır. Bu hizmetler birden fazla insandan işlem kabul edip aktarılan kaynakları küçük meblağlara bölerek ve bunları hizmetin diğer kullanıcıları tarafından aktarılan kaynaklarla karıştırarak çalışmaktadır. Bu da şu anlama gelmektedir; kaynakların alıcısının gözünden bakıldığında, kaynakların orijinal kaynağı en azından aşırı derecede perdelenmekte ve muhtemelen bütünüyle anonimleştirilmektedir¹¹¹.

5.4.4 Gelirlerin Nakde Çevrilmesi / Tahakkuku ve Tahvili

Sanal para birimleriyle ifade edilen değerın itibarı para birimine dönüştürüldüğü noktada, kolluk kuvvetlerinin devreye girme ihtimali bulunmaktadır. Bu dönüştürme tipik olarak bir sanal para birimi takasında gerçekleşmektedir, dolayısıyla Bölüm 5.3 altında kısaca tartışılmış olan ve atıfta bulunulan sanal para birimleri ile ilgili MEGG tavsiyeleri, sanal para birimi düğümlerinin düzenlemeye tabi kılınmasına odaklanmaktadır. Bu bağlamda "düğümler" sanal para dünyasının geleneksel finans dünyasına dokunduğu, başka şeylerin yanında, sanal para birimi takasını içeren noktalara atıfta bulunmaktadır.

Sanal para birimi takaslarının düzenlemeye tabi kılındığı yerlerde, bu hizmetleri verenlerin müşterilerinin kimliklerini tespit etmek için gerekli özeni göstermesi zorunludur. Bitcoin özel örneğinde, tüm işlemler blok zincirinde herkese açıktır. Bu da şu anlama gelmektedir; kolluk kuvvetlerinin bir şüpheli kontrolü altında olan belirli bir sanal para birimi adresinin farkında olduğu durumlarda, belirli bir sanal para birimi takasının kullanımını belirlemek, şüpheli tarafından gerçekleştirilen işlemlerin analiz edilmesi ile mümkün olabilmektedir. Bu örneklerde, kolluk kuvvetleri, müşteri kimlik bilgileri, ev adresi, İP adresleri, e-posta adresleri, telefon numarası, işlem geçmişi, para yatırma ve para çekme adresleri, banka adı, banka hesap numarası ve işlem bilgileri gibi müşteri detaylarını ortaya çıkarmak üzere ilgili sanal para birimi takasına mahkeme emri ile gidebilmektedir.

¹¹⁰Kara para aklama ve terör finansmanı karşıtı mevzuat çerçevesinde uygunluk gösteren kuruluşlar sanal para birimi takasçıları, ödeme işlemcileri kurumları, çevrimiçi cüzdanlar, kumar siteleri ile sınırlı değildir ve diğer internet hizmetleri de soruşturmalara yardımcı olabilmektedir.

¹¹¹https://en.bitcoin.it/wiki/Mixing_service

Örneğin, Ocak 2016'da, internet üzerindeki yasadışı uyuşturucu pazarlarına yapılan uluslararası bir baskının parçası olarak Hollanda'da on erkek tutuklanmıştır. Bu kişiler, Bitcoin'lerini ticari Bitcoin hizmetleri kullanarak banka hesaplarında Avro'ya dönüştürüp ardından ATM'lerden nakit olarak milyonlar çekerken yakalanmışlardır. Bitcoin adreslerinin izi sürülerek, bu paralarla FBI ve Interpol tarafından izlenen internet üzerindeki yasadışı uyuşturucu satışları arasındaki bağlantının bulunduğu iddia edilmiştir. MEGG, Sanal Para Birimleri 2014 raporunda ("Sanal Para Birimleri: Kilit Tanımlamaları ve Kara Para Aklama Karşısı Önlemler ve Terörizmin Finanse Edilmesi ile Mücadele Açısından Ortaya Çıkan Potansiyel Riskler"), sanal para birimlerini içeren, kamuya gayet iyi anlatılmış, bazı başka kolluk kuvveti eylemlerine ilişkin örnekler sunmaktadır.¹¹² İlgili okurun, sanal para birimlerini içeren daha önceki soruşturmaların ölçeği ve karmaşıklığı hakkında daha fazla bilgi almak için bu vaka çalışmalarını gözden geçirmesi teşvik edilmektedir.

Ancak, bu kılavuzun başka yerlerinde tartışıldığı gibi, sanal para birimlerinin küresel niteliği dolayısıyla güçlükler yaşanmaya devam etmektedir. Bu güçlükler geniş bir yelpazeye yayılmaktadır; dünya genelinde sanal para birimi takaslarının tutarlılık gösteren bir biçimde düzenlemeye tabi kılınmamasından tutun, uluslararası soruşturmalarla ilgili pratik zorluklara kadar.

5.5 Dondurma/ Zapt Etme Konusundaki Güçlükler

5.5.1 Suç Gelirleri Olarak Sanal Para Birimleri

Birçok ülke suç gelirlerinin niteliğini belirtmek zorunda değildir. Bu örneklerde, kazançlar suç faaliyetinden türetilmişse, Bitcoin gibi bir değer deposu suç geliri olarak kabul edilmelidir. Bununla birlikte, bunun sizin hususi yargı yetkisi alanınızda saptanması gerekmektedir.

5.5.2 Sanal Para Biriminin Varlığının Saptanması

İlk zorluk, sanal paranın varlığını tespit etmek ve bunun şüpheli tarafından kontrol edildiğini belirlemektir. Burada ortaya çıkan bazı konular Bölüm 5.4'te halihazırda tartışılmıştır. Sanal paranın varlığı ve kontrolü, örneğin, izleme, özel araştırma teknikleri ve hatta kabullerden anlaşılabilir.

5.5.3 Sanal Para Biriminin Dondurulması / Denetiminin Ele Geçirilmesi

Suç gelirlerinin sanal para birimi şeklinde tutulduğunu belirledikten sonra, bir sonraki soru, sanal para birimini hareketsiz kılmak ve yayılmasını önlemektir. Sanal para biriminin dondurulmasında karşılaşılan güçlük bir açıdan sanal nitelikli olmalarıdır; yani sanal para cüzdanının birçok kopyasının var olabilmesidir. İnternetteki bir cüzdanın veya bir şüphelinin bilgisayarında tutulan bir cüzdanın zapt edildiği durumlarda bile, sanal paranın şüpheli kontrolünün dışına taşındığından emin olmak için yeterli zemine kavuşulmuş olmamaktadır. Bir şüphelinin bulut (internet depolama alanı) üzerinde, başka yerde tuttuğu yedek anahtarları / cüzdanı olması nadiren rastlanan bir durum değildir. Bu nedenle, bir şüphelinin sanal para cüzdanının kontrolünü ele geçirme denemeleri, varlıkların şüpheli kontrolünün dışına taşındığı konusunda kesinlik sağlayamamaktadır.

Sanal para birimlerinin bu bakımdan bir cihazda saklanmadığı vurgulanmalıdır. Bitcoin'ler örneğinde, kişinin onları harcamasına izin veren özel anahtardır. Bitcoin'leri zapt etmenin

¹¹²MEGG Raporu, Sanal Para Birimleri Kilit Tanımlamaları ve Kara Para Aklama Karşısı Önlemler ve Terörizmin Finanse Edilmesi ile Mücadele Açısından Ortaya Çıkan Potansiyel Riskler, Haziran 2014. Ulaşmak için bkz.: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

başlıca iki yolu bulunmaktadır; şüphelinin özel kilidine erişim sağlamak ya da şüphelinin özel kilidini kontrol eden özel sektör kuruluşuyla (örneğin, takaslar) işbirliği yapmak. Soruşturma görevlileri zapt etme işlemini tamamlamak için şüpheli özel kilidine sahip olduklarında, şüpheli veya özel kilidi kontrol eden bir başka kişinin fonları başka bir adrese taşıyabilme olasılığı olduğundan, yapılması gereken fonları aktarmak olacaktır. Bunlar, kolluk kuvvetlerince (soruşturma görevlileri veya savcılık) kontrol edilen bir Bitcoin adresine aktarılmalıdır. Bu prosedürün mevcut ulusal mevzuata yaslanacağını unutmayın.

Bir savcı, şüpheli veya temsilcilerinin sanal para birimini yaymasını engelleyen yasal bir tedbir veya ayrı bir dondurma emri alabilir. Bu, emrin hiçbir etkisinin olmayacağı denizaşırı ülkelerde bulunan temsilcileri sanal paranın yerini değiştirmek veya sanal parayı yaymak için harekete geçmekten alıkoymaz.

Eğer mümkünse, kovuşturma, sanal para birimi bakiyesini mümkün olan en kısa sürede likide etmelidir (bkz. Bölüm 5.5.4). Bu, bir şüphelinin hedef sanal para birimi cüzdanının bir kopyasına erişimi olması durumunda, varlıkların kontrolünü ele geçirmek konusunda işlemlerin zamanında yürütülmesini zorunlu hale getirmektedir. Ek olarak, sanal para birimleri genellikle değer bakımından uçucudur ve bakiyeyi likide edip bir hükümet hesabına koyarak, soruşturma sırasında sanal para biriminin temsil ettiği değeri koruyacağınızdan ve mahkûmiyet durumunda nihai müsadere için söz konusu değerini erişilebilir olacağından emin olabilirsiniz.

5.5.4 Varlık Yönetimi

Tavsiye edilen en iyi uygulama sanal para birimi değer deposunu likide etmektir. Bunun nedeni müsadere edilen malların değerini koruma ihtiyacıdır (örneğin zapt edilen tahviller ve nakit dövizde aynı durum geçerlidir). Bu, varlığın değerinin korunmasını ve piyasadaki uçuculuğa karşı savunulmasını sağlamaktadır. Ayrıca sanal para biriminin hareket ettirilemeyeceği, aktarılamayacağı veya mahkemelerin erişimi dışına çıkarılamayacağı konusunda yeniden güvence sağlamaktadır. Pek çok yargı yetkisi alanı, nihai müsadere için değerlerin korunması adına varlıkların likide edilmesini öngören hükümleri mevzuatlarında taşımaktadır fakat bunun sizin hususi yargı yetkisi alanınızda belirlenmesi gerekecektir.

AB Müsadere Direktifi¹¹³ zapt edilen ve müsadere edilen varlıkların yönetimi için bir ofis kurulmasını tavsiye etmektedir¹¹⁴. Eğer sizin yargı yetkisi alanınızda bu türden bir ofis kurulursa, bu ofisin bir sanal para birimi değeri stokunu nakde çevirme kapasitesi konusunda bilgi edinmeniz değerli olabilir. Alternatif olarak, eğer böyle bir ofis bulunmuyorsa, sanal para birimi değerini nakde çevirme becerisi, müsadere öncesi varlıkları yönetmek konusunda yürürlükte olan hangi düzenlemelerse o düzenlemelerin kapasitesine bağlı olacaktır.

ÜZERİNE DÜŞÜNÜLECEK SORULAR

1. Sanal para birimini mümkün olan en kısa sürede nakde çevirmek neden en iyi uygulamadır?
2. Sizin yargı yetkisi alanınızda belirli suç gelirlerinin yasadışı kaynağını tespit etmek zorunlu mudur? Eğer öyle ise, bu sanal para birimi söz konusu olduğunda nasıl gerçekleştirilebilir?

¹¹³Avrupa Birliği'nde suç vasıtalarının ve gelirlerinin dondurulması ve müsadere ile ilgili, 3 Nisan 2014 tarihli, 2014/42/EU sayılı Avrupa Parlamentosu ve Konsey Direktifi.

¹¹⁴*Ibid* Giriş paragraf 32.

3. Sanal para birimini zapt etme emrinin alınabilmesi için hangi şartların oluşması gerekmektedir?
4. Sanal para birimlerinin varlığını veya kullanımını saptamak için ne türden önlemler alınabilmektedir? Masum üçüncü tarafların çıkarlarını korumak için yürürlükte geçerli olan emniyet tedbirleri nelerdir?

6 Pratik Çalışma / Vaka Çalışmaları

6.1 Literatür Taraması

Lütfen, aşağıdaki hususları göz önünde bulundurarak, kısa bir açıklamayla, ulusal mevzuatınızdaki ilgili maddeleri ve ilgili içtihatları içeren bir referans listesi hazırlayınız:

1. Ceza Kanunu ve Ceza Muhakemeleri Usul Kanunu / özel kanun çerçevesinde bir yükümlülük olarak suç gelirlerinin müsadere.
2. Mali soruşturmanın tanımı, bir mali soruşturma ne zaman gerçekleşmelidir, bir mali soruşturmayı kim yürütür?
3. Banka verilerine erişim ve bir banka hesabının izlenmesi.
4. Özel soruşturma önlemlerinin tanımlanması ve kullanımı.
5. Diğer mülkiyet veri tabanlarına erişim (tapu kaydı, araba tescili vs.)
6. Dondurma emri.
7. Müsadere kararı.
8. Müsadere rejimi (ceza yargılaması, değer tabanlı müsadere, genişletilmiş müsadere, muvazenesizlik varsayımı, mahkûmiyet kararı (aynı) gerektirmeyen müsadere).
9. Hukuki yardımlaşma.
10. Uzmanlaşmış kurumlar.
11. Bir Görev Gücü yaratılması (kovuşturma, polis, MİB, vergi kurumları, gümrük).
12. Abone verilerine erişim (İP adresi, internet sayfası, e-posta hesabı).
13. Akış verilerine ve içerik verilerine erişim.
14. Muhafaza talebi.
15. Elektronik kanıtların zapt edilmesi.

6.2 Vaka çalışması 1: Önlemin Hukuki Temeli Üzerine Düşünme

Ulusal polisiniz D ve E alıcılarına büyük miktarlarda esrar satmak için organize bir suç grubu kuran A, B ve C şüphelilerine karşı bir soruşturma başlattı.

Örtülü önlemler kullanarak (örtülü izleme ve telekomünikasyon izlemesi), 15 Ekim 2016 tarihinde A kişinin D kişisine 1 kg esrar teslim ettiği saptanmıştır. D kişisi, bir çanta içinde 1.000 Avro nakit ödemiştir. Zapt etme ve tutuklamanın ertelenmesine izin verilmiştir. Aynı gün, A kişisi B kişisine paralı çantayı teslim etmiştir. Ayrıca A kişinin E kişisiyle telefonda konuşarak ona 2 kg. esrar satmayı kabul ettiği ve bu esrara karşılık 11 numaralı banka hesabına 2.000 Avro havale edildiği saptanmıştır.

11 numaralı banka hesabının sahibi ile ilgili verilere, hem hesap sahibi hem de son X aydır yapılan işlemlerle ilgili verilere erişmeniz gerektiğine karar veriyorsunuz. Ayrıca, A, B ve E kişilerinin hesapları için işlemlere yönelik izleme başlatılması gerektiğine karar veriyorsunuz.

SORU: Belirli maddelere atıfta bulunarak, ulusal mevzuatınızdaki yasal temeli ve banka verilerine, işlem verilerine erişim ile hesapların izlenmesinin koşullarını açıklayınız.

Bu önlemlerle A, B ve E'nin tamamının sizin ülkenizde banka hesapları olduğunu saptıyorsunuz. Aynı zamanda B'nin Avusturya'da bir banka hesabı olduğunu saptıyorsunuz.

Banka verileri, işlem verileri ve B'nin Avusturya'daki hesabının izlenmesi için mahkeme emri çıkarttırmaya ve hukuki yardımlaşma talebinde bulunmaya karar veriyorsunuz.

SORU: Belirli maddelere atıfta bulunarak, ulusal mevzuatınızdaki yasal temeli ve hukuki yardımlaşma koşullarını açıklayınız.

A, B ve E'nin banka hesaplarının incelenmesi yoluyla, A ile B arasında, E'den B'ye ve B'den de yurtdışına (bölgedeki bir başka ülkeye ve ayrıca Lüksemburg'a) sık sık işlemler gerçekleştiği açıkça ortaya çıkıyor. Ceza soruşturmasının bulgularıyla işlemlerin dinamiklerini karşılaştırıyor ve ilişkilendiriyorsunuz.

Telefon izlemesi, B'nin, sizin ülkeniz ile bölgedeki bir başka ülke arasında ikamet eden C ile, bir aylık bir süre zarfında, 15 Aralık 2016 günü için daha yüksek miktarda esrar tedariki pazarlığı yaptığını ortaya seriyor. C, 22 numaralı banka hesabına (tüzel kişi DOO'nun hesabı), 1 Aralık 2016 öncesinde ücretin yarısını (100.000 Avro) içeren bir ön ödemenin yapılmasını, geri kalan 100.000 Avro'nun Lüksemburg'daki bir bankadaki 33 numaralı banka hesabına ödenmesini istiyor.

C'nin ülkenizdeki ve bölgedeki diğer ülkedeki banka hesapları hakkında veri edinmeye ve bir izleme emrini yürürlüğe koydurmaya karar veriyorsunuz. Ayrıca tüzel kişi DOO'nun ve banka hesaplarının sahibini saptamaya ve son X aydır gerçekleşmiş olan işlemlerle ilgili verileri ve DOO'nun hesaplarının izlemeye alınmasını talep etmeye karar veriyorsunuz.

SORU: Maddelere atıfta bulunarak, ulusal mevzuatınızdaki yasal temeli ve tüzel kişiler, tüzel kişilerin banka ve işlem verileri, tüzel kişilerin vergi kayıtları ile ilgili verilere erişimin şartlarını açıklayınız.

Vergi kurumlarının yardımıyla, DOO'nun nasıl iş yürüttüğünü ve iş ortaklarının kimler olduğunu saptamaya karar veriyorsunuz. DOO'nun sınıai kenevir ticareti de yaptığını keşfediyorsunuz.

Lüksemburg'daki 33 numaralı banka hesabının kayıtlarını talep ediyorsunuz ve bu hesabın sizin ülkenizde ve C'nin mülkiyetindeki bir tüzel kişiye ait olduğunu görüyorsunuz.

SORU: Burada kara para aklama şüphesi var mı? Hangi noktada şüphe ortaya çıkıyor? Soruşturma görev gücüne MİB'i dâhil etmeli misiniz? MİB'in ne konuda yardımı dokunabilir? Burada hangi olası kara para aklama tipleri gündemdedir? Kara para aklama konusunda, ulusal mevzuatınızdaki yasal temeli, unsurları ve şartları açıklayınız. MİB ile ilişkilendirme konusunda, ulusal mevzuatınızdaki yasal temeli ve şartları açıklayınız.

Telefon izlemesi B kişinin, uyuşturucu alışverişleri ve Bitcoin cinsinden ödemeler ile ilgili bilgiler içeren, A kişisi ile gerçekleştirdiği e-posta iletişimine atıfta bulunduğunu saptıyor.

A kişisi ve B kişisi tarafından kullanılmakta olan e-posta adreslerini ve e-postaların içeriğini saptamanız gerektiğine karar veriyorsunuz. A kişinin yerel bir internet hizmeti sağlayıcısı tarafından sağlanan bir e-posta adresini kullandığını saptıyorsunuz.

SORU: Maddelere atıfta bulunarak, ulusal mevzuatınızdaki yasal temeli ve İSS'ler ile işbirliği ve e-posta içeriklerine erişim şartlarını açıklayınız.

A'nın e-posta içeriği üzerinden, D, E ve diğerlerine uyuşturucu satıldığını, ayrıca banka hesaplarına nakit havale ve aynı zamanda Bitcoin cinsinden değer aktarımı yapıldığını saptıyorsunuz.

Banka işlemlerini analiz etmek ve bağlantıları, yurtdışındaki (Avusturya ve Lüksemburg ile bölgenizdeki diğer ülkelerdeki) ilgili hesapların sahipleri hakkındaki verileri araştırmak üzere MİB'in yardımına başvurmaya karar veriyorsunuz.

SORU: Maddelere atıfta bulunarak, ulusal mevzuatınızdaki yasal temeli ve MİB tarafından banka verilerine erişim ve uluslararası MİB işbirliği şartlarını açıklayınız.

Soruşturma neticesinde 15 Aralık 2016 tarihinde C kişisinden B kişisine bir ödeme yapılacağını saptıyorsunuz. B'nin Bitcoin cüzdanının Lüksemburg'daki bir Bitcoin takasında olduğunu saptıyorsunuz.

SORU: Maddelere atıfta bulunarak, ulusal mevzuatınızdaki yasal temeli ve bir Bitcoin takasından abone bilgisi talep etmenin şartlarını açıklayınız. Ülkenizdeki bir Bitcoin takası verileri tutmaya ve işbirliği yapmaya yükümlü olur muydu?

SORULAR:

- Tüzel kişi DOO'nun 22 numaralı hesabına 1 Aralık 2016'da yapılması planlanan ödeme ile ilgili olarak hangi önlemleri alacaksınız?
- Önden işlem dondurma emri verecek misiniz? Dondurma emri ne zaman ifşa edilir? DOO'nun hesabı üzerindeki işlemlerin dondurulması, 15 Aralık 2016 tarihinde teslimatı öngörülen büyük miktarda uyuşturucunun ele geçirilmesini tehlikeye düşürür mü?
- Şüpheliler tutuklandıktan sonra, 15 Aralık 2016 tarihli nakit ödeme ile ilgili olarak hangi önlemler alınır?
- A, B ve C grubunun uzun süredir uyuşturucu işinde olması göz önünde bulundurulduğunda, ne tutarda ve hangi varlıklar müsadere edilebilir? Yanıtınız için ulusal mevzuatınızdaki temeli açıklayınız.
- DOO tüzel kişisi uyuşturucu kaçakçılığı ve/veya kara para aklama ile suçlanabilir mi? Eğer öyleyse, ulusal mevzuatınızdaki yasal temeli ve bir tüzel kişiyi cezaya çarptırma şartlarını açıklayınız. Tüzel bir kişiden müsadere yapılması ile ilgili bir karar ve yargılama örneğini açıklayınız.

B ile A arasındaki e-posta iletişimini analiz ederek, grubun karanlık ağda belirli bir internet sayfası üzerinden de uyuşturucu sattığını keşfediyorsunuz. Bu, alıcılardan birisi tarafından doğrulanıyor ve alıcı sorgu sırasında karanlık ağda siparişlerin ve uyuşturucu sevkiyatının nasıl işlediğini ve ödemelerin banka hesabına veya Bitcoin ile yapılmasının nasıl talep edildiğini ortaya seriyor¹¹⁵.

SORU: Karanlık ağ faaliyetleri ile ilgili kanıtlarla alakalı olarak eylemlerinizi neler olur? Bir alıcı olarak örtülü soruşturmaya girişip uyuşturucu satın alır, ilgili banka hesaplarını ve Bitcoin cüzdanlarını keşfedip para ve mülkleri dondurabilir misiniz?

¹¹⁵Örneğin bkz.: <https://www.bitstamp.net/help/what-is-bitcoin/>

6.3 Vaka çalışması 2: Mali İstihbarat Birimi / Kolluk Kuvvetleri Etkileşimi Üzerine Düşünme

Ülkenizdeki Mali İstihbarat Birimi (MİB) bir bankadan internet bankacılığı üzerinden gerçekleşen bazı işlemlerden şüphelendiklerini belirten bir rapor alıyor. Kurum, bazı müşteri hesaplarına büyük meblağların havale edildiğini ve bu meblağların ilgili müşteriler için tipik sayılamayacağını saptamıştır. Ek olarak, mali kurum, müşterilerinin Romanya'daki İP adreslerinden internet bankacılığına giriş yapmış görüldüğünü gözlemlemiştir ki müşterilerden hiçbirisi daha önce bu ülkeden giriş yapmamıştır. Bu hareket toplam 20 müşteri hesabında gözlemlenmiş ve 20 hesaptan gelen toplam değer 750.000 Avro'dur.

MİB bir analiz gerçekleştirip başka bankaların müşterilerinin hesaplarından geçen şüpheli işlemler gösteren, başka şüpheli işlem raporları tespit eder. MİB bir rapor hazırlayıp bu raporu polise iletir.

Polis istihbaratı araştırması, sahte kimlik belgeleri ile ilişkili olarak Romanyalı şahısları (gerçekte Moldovalı ama sizin ülkenizde ikamet ediyorlar) konu alan mevcut bir polis soruşturması saptar.

Polis şahısları tutuklar, kaldıkları binaları arar ve bazı dizüstü bilgisayarlara el koyar. Dizüstü bilgisayarların adli incelemesi bunların 200'ü aşkın banka hesabı üzerinde kontrol sağlamak üzere kullanıldığını, bu banka hesaplarının ise bilgisayarlarına banka hesabı bilgilerini ele geçiren Truva "Dridex"¹¹⁶ bulaşmış bireylerin banka hesaplarından elde edilen parayı almak ve aklamak üzere kullanıldığını gözler önüne serer. Bu hesaplar üzerinden aklanan toplam meblağ 3 milyon Avro'nun üzerindedir.

Şüphelilere dava açılır ve sırasıyla 8 ve 5 yıl hapis cezası alırlar. Herhangi bir suç geliri geri kazanılmamıştır.

SORU: MİB'in durumu polise raporlamasının yasal temeli nedir?

Bu etkileşimin bir yasal temeli olabilir, ancak pek çok örnekte, polis ve MİB (ve vergi kurumları, gümrük vs. türünden diğer kurumlar) bilgi paylaşımının gerçekleşebilmesi için bir Mutabakat Anlaşması imzalar. Yasal temel, polise sunulan raporun niteliğine de bağlı olabilir. Örneğin, polise gönderilerin bilgiler (polis tarafından) istihbarat bilgileri olarak görülebilir veya bir suç ihbarı olarak görülebilir.

Lütfen kendi ülkenizdeki durumu araştırın.

SORU: Sizin ceza muhakemeleri usul kanununuzdaki hangi hükümler polis araştırmasına ilişkindir?

Siber suçlar, mali soruşturmalar ve kara para aklama alanıyla ilgili olarak, bu örnek senaryoda polisin aldığı bazı önlemler bulunuyor; nesneler ve binalar aranıyor, dizüstü bilgisayarlara el konulup bunlar adli olarak inceleniyor, gizliliği ihlal edilmiş banka hesaplarından kanıtlar toplanıyor.

¹¹⁶Dridex esas itibarıyla bankacılık bilgilerini çalmak için kullanılan saldırgan bir truva. Bu kötü amaçlı yazılım 40'l aşkın bölgede yaklaşık 300 farklı kuruluşun müşterilerini hedef alacak şekilde ayarlanmıştır. Dridex ağırlıklı olarak zengin, İngilizce konuşulan ülkelerdeki mali kurumların müşterilerine odaklanmaktadır, hedefe konulan kuruluşların büyük çoğunluğu bu ülkelerdedir. Saldırganlar Asya-Pasifik coğrafyasından bir dizi bölgenin yanı sıra diğer Avrupa uluslarına da öncelik vermektedir.

Bu sorunun amacı bu türden eylemler bakımından sizin ceza muhakemeleri usul kanununuzdaki yasal temel üzerine düşündürmektir.

SORU: Sizin ceza yasanızın hangi hükümleri bir müşterinin bilgisayarına virüs bulaştırılmasını suç haline getirmektedir?

Eğer ülkeniz Budapeşte Sözleşmesi'ni onaylamışsa, o zaman bir bilgisayara virüs bulaştırılmasına suç muamelesi yapılacaktır. Budapeşte Sözleşmesi'nden ilgili maddeyi aktaran sizdeki Ceza Yasası hükmü nedir?

Eğer ülkeniz Budapeşte Sözleşmesi'ni onaylamamışsa, eşdeğer hükümlerinizi var mı? Bilgisayar suçlarına nasıl suç muamelesi yapılıyor?

SORU: Truva Dridex faaliyetini zanlılara nasıl bağlarsınız?

Şüpheliler internet bankacılığı bilgilerini toplamak için kötü amaçlı bir yazılım kullanmıştır. Ancak, bu bilgiler mağdurların bilgisayarlarından toplanacaktır, şüphelilerin bilgisayarından değil. Dolayısıyla, Truva'nın faaliyetini şüphelilere nasıl bağlayabilirsiniz? Gizliliği ihlal edilen banka hesabı detaylarına sahip olunması (bu, şüphelilerin dizüstü bilgisayarlarında var olmaları üzerinden saptanabilir) ile bu hesap detaylarının gizliliğinin Truva ile ihlal edilmesi arasında nedensel bir bağlantı kurabilir misiniz? Eğer yanıtınız evet ise, buna nasıl yaklaşırsınız? Eğer yanıtınız hayır ise, şüphelilerin sorumlu tutulabileceği suçlamalar açısından bunun ne gibi sonuçları olur?

SORU: Romanyalılar/Moldovalılar, paranın havale edildiği banka hesaplarını kontrol edenler ve virüsü yayan kişi arasında bağlantıları nasıl kurabilirsiniz? Şüphelilerin (sizin ülkenizde veya yurtdışında) mülkleri olup olmadığını nasıl tespit edebilirsiniz?

Bir önceki sorudan devam edersek, şüphelinin dizüstü bilgisayarındaki banka hesabı detaylarının varlığı, şüphelilerin söz konusu paranın havale edildiği anda banka hesaplarının kontrolüne sahip olduğunu gösterebilir de göstermeyebilir de. Bunun ayrıca mı tespit edilmesi gerekir, yoksa banka hesaplarına sahip olunmasından bu sonuç çıkarılabilir mi?

SORU: Bilgisayar destekli hırsızlık için kovuşturma yapabilir misiniz?

Bu örnekte bilgisayarlar hırsızlığın temel bir bileşeni olarak kullanılmıştır. Ulusal mevzuatınızda bilgisayarların hırsızlık/dolandırıcılık davalarında bir araç olarak kullanılmasına suç muamelesi yapan bir hüküm bulunuyor mu?

SORU: Ulusal mevzuatınızdaki hangi usul hükümleri elektronik kanıtların toplanmasını ve kullanılmasını düzenlemektedir?

Bunun gibi davalarda, şüphelilerin dizüstü bilgisayarlarından elde edilen kanıtlar son derece önemli olabilir. Dolayısıyla, sizin ulusal mevzuatınızdaki elektronik kanıtların toplanmasını ve kullanılmasını düzenleyen hükümler nelerdir?

SORU: Ülkenizin bir adli bilgisayar kapasitesi var mı? Adli bilgisayar kapasitesi ile nasıl ilişki kuruyorsunuz?

Pratik açıdan bakıldığında, elektronik kanıtların toplanması ve yönetimi özelleşmiş araçlar ve beceriler gerektirir. Bu sizin ülkenizde nasıl düzenleniyor?

SORU: Bu örnekte bir mali soruşturma yürütülmeli midir? Mali soruşturma hangi noktada başlatılmalıdır?

Senaryoda betimlendiği haliyle, şüphelilerin faaliyetiyle bağlantılı açıkça çok önemli mali sonuçlar var. Ülkenizde, bu örnekte bir mali soruşturma yürütülür mü (yürütülmesi gerekir mi)? Eğer evet ise, mali soruşturma hangi noktada başlatılmalıdır?

SORU: Bu örnekte ulusal mevzuatınızdaki hangi hükümler varlıkların aranmasını, zapt edilmesini ve müsaderesini düzenlemektedir? Çalınan parayı nasıl geri alırsınız? (MİB veya polis/savcı yardımıyla) Dondurabilir misiniz?

Senaryo şüphelilerin hapis cezaları aldıklarını gösteriyor. Ulusal hükümlerinizi, ceza kovuşturması sonrasında kovuşturmanın varlık müsaderesi bileşenini zorunlu kılıyor mu, yoksa bunlar tek bir kovuşturmada mı gerçekleşiyor?

Dolandırılan mağdurların çalınan kaynaklarını geri alma ihtimali var mı? Paranın bir bölümünü veya tamamını geri alırsanız, mağdurları tazmin eder misiniz? Ulusal mevzuatınızdaki hangi hükümler bunu kolaylaştırıyor?

SORU: Ulusal mevzuatınızdaki hangi hükümler kara para aklama suçunu tanımlamaktadır? Bir kara para aklama suçu söz konusu mudur?

Ulusal mevzuatınızda kara para aklama suçu nasıl tanımlanıyor? Senaryoda anlatılan olgular göz önünde bulundurulduğunda, bir kara para aklama suçu söz konusu mudur?

SORU: Hırsızlık/dolandırıcılığın yanı sıra kara para aklama suçu için de kovuşturma yapar mısınız? Neden evet / neden hayır?

Bu dava düşünüldüğünde, Hırsızlık/dolandırıcılığın yanı sıra kara para aklama suçu için de kovuşturma yapar mısınız? Evet ise, neden? Hayır ise, neden?

SORU: Mağdurlar birden fazla ülkeye yayılmış durumdadır, soruşturmanızda bu ülkelerle nasıl koordinasyon kurarsınız?

İnternetin sınır tanımayan doğası nedeniyle, siber suç bileşeni olan neredeyse tüm davalar aynı zamanda bir uluslararası yan taşımaktadır. Bu örnekte, eğer birden fazla ülkede mağdur varsa, söz konusu diğer ülkelerle koordinasyon kurar mısınız? Peki ya soruşturmanız üzerinden daha önce bilinmeyen daha fazla mağdur olduğunu tespit ederseniz?

SORU: Kanıt sunmak için süre sınırınız var mı ve hukuki yardımlaşma istekleri bu sınırları aşıyor mu? Hukuki yardımlaşma taleplerinde gecikmeleri nasıl azaltırsınız?

Eğer işin içine karışan bir uluslararası yön varsa, hukuki yardımlaşma sürecine başvurma ihtiyacı oluşabilir, bu da soruşturmada önemli gecikmelere neden olabilir. Hukuki yardımlaşma sürecindeki süreler ülkenizdeki soruşturmalar için günlük yaratır mı? Sürelerdeki uzamalar nasıl azaltılabilir? Örneğin, ortak soruşturma ekipleri kullanabilir misiniz? Hukuki yardımlaşma istekleri öncesinde gayri resmi iletişim kanallarını kullanabilir misiniz?

6.4 Vaka çalışması 3: Siber Suç / Kara Para Aklama Etkileşimi Üzerine Düşünme

Ülkenizdeki pek çok yurttaş bilgisayarlarına tüm fotoğraflarını ve dokümanlarını şifreleyen, kötü amaçlı bir yazılım bulaştırdığını bildiriyor. Kötü yazılım ardından fotoğraf ve dokümanların şifresini çözmek için Bitcoin cinsinden bir ödeme talep ediyor. Bazı örneklerde yurttaşlar fidyeyi ödemiş durumda.

Soruşturma sırasında, polis, Bitcoin izlenmesine yardımcı olması için MİB ile ilişkililiyor. MİB bitcoin'lerin itibari paraya çevrildiği takasa kadar bitcoin'lerin izini sürebiliyor. Bitcoin takasının yeri Birleşik Devletler'de.

Birleşik Devletler'e bir hukuki yardımlaşma talebi gönderiliyor ve işlemleri gerçekleştiren hesapların detayları talep ediliyor. Birleşik Devletler'den yanıt alınınca, Bitcoin karşılığının sizin ülkenizdeki İP adreslerini kullanan bireyler tarafından sizin ülkenizdeki banka hesaplarına havale edildiği ortaya çıkıyor.

SORU: Şüphelileri (İP adresini) nasıl tespit edersiniz? Bu verileri nasıl elde edersiniz; ulusal düzeyde mi, yurtdışından mı? İP adresleri sizin ülkenizde değilse ne olur?

Bir İP adresi ile bir geçek dünya kişisi arasındaki bağlantı, internet soruşturmalarının en önemli yönlerinden birisidir. Eğer İP adresi ülkenizde ise, bu veriye erişim sağlamak üzere ulusal internet hizmeti sağlayıcıları ile nasıl ilişkilirsiniz? Hangi yasal hükümler bu erişimi olanaklı kılar? Bu veriyi muhafaza etmeleri ve erişilebilir kılmaları için internet hizmeti sağlayıcılarına yüklenen yükümlülükler nelerdir?

İP adresinin ülkenizde olmadığı durumu düşünün. Farklı olan nedir? Bu örnekte duruma nasıl yaklaşırsınız?

SORU: Banka hesabı sahipleri (senaryoda paragraf üç), Bitcoin cüzdanı sahipleri ve kötü amaçlı yazılımı kullanan kişiler arasındaki ilişkiyi nasıl kurabilirsiniz? Bu örnekte bir mali soruşturma yürütülmesi gerekir mi?

Hukuki yardımlaşma talebine gelen yanıt Bitcoin'in itibari paraya dönüştürülmesinde kullanılan İP adreslerini ve banka hesabı detaylarını gösteriyor. (a) Eğer hâlihazırda bilmiyorsanız, hesabın hangi mali kurumda olduğunu nasıl öğrenirsiniz ve (b) banka hesabı sahibi hakkında bilgi edinmek için mali kurum ile nasıl ilişkiye geçersiniz? Bu erişimi olanaklı kılan hangi yasal hükümlerdir? Bu veriyi muhafaza etmeleri ve erişilebilir kılmaları için mali kurumlara yüklenen yükümlülükler nelerdir?

Tekrar banka hesaplarının bir başka ülkede olduğu durumu düşünün. Bu örnekte farklı olan nedir ve duruma nasıl yaklaşırsınız?

SORU: Bir mali soruşturma başlatılmalı mıdır, eğer başlatılmalı ise, hangi noktada başlatılmalıdır?

Senaryoda anlatıldığı gibi, şüphelilerin faaliyetiyle bağlantılı önemli mali çıkarımlar söz konusudur. Ülkenizde, bu örnekte bir mali soruşturma yürütülür mü (ve yürütülmesi gerekir mi)? Eğer evet ise, mali soruşturma hangi noktada başlatılmalıdır?

SORU: Ulusal mevzuatınızdaki hangi hükümler kara para aklama suçunu tanımlıyor? Bir kara para aklama suçu söz konusu olmuş mudur?

Sizin ulusal mevzuatınızda kara para aklama suçu nasıl tanımlanıyor? Senaryoda anlatılan dava olgularını göz önünde bulundurduğunuzda, bir kara para aklama suçunun söz konusu olduğunu söyleyebilir misiniz?

SORU: Senaryo, Bitcoin faaliyetini çözümllemek ve izini sürmek konusunda polis ve MİB'in ortak faaliyette bulunmasını anlatıyor. Bu tip bir işbirliğinin yasal temeli nedir?

Bu etkileşimin bir yasal temeli olabilir, ancak pek çok örnekte, polis ve MİB (ve vergi kurumları, gümrük vs. türünden diğer kurumlar) bilgi paylaşımın gerçekleşebilmesi için bir Mutabakat Anlaşması imzalar.

Lütfen kendi ülkenizdeki durumu araştırın.

SORU: Ülkenizde sanal para birimleri, özel olarak da Bitcoin nasıl düzenlenmekte?

Bitcoin ile ilgili olarak dünya genelinde çeşitli düzenleyici rejimler bulunmaktadır. Sizin ülkenizde durum nedir?

SORU: Ülkenizde sanal para birimleri yükümlü kuruluşlar mı, şüpheli işlemleri raporlama zorunlulukları var mı?

Özel olarak, takaslar veya cüzdan hizmetleri türünden sanal para birimi kuruluşları üzerinde şüpheli faaliyetleri raporlama yükümlülüğü var mı?

7 Ek: İlgili Okumalar Listesi

7.1 Avrupa Konseyi

- Convention on Cybercrime, ETS 185, 23.11.2001: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
[Siber Suçlar Sözleşmesi, Avrupa Anlaşma Serisi 185, 23.11.2001]
- Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189, 28.01.2003: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>
[Bilgisayar sistemleri üzerinden işlenen, ırkçı ve yabancı düşmanı nitelikli eylemlerin suç olarak kabul edilmesine ilişkin, Siber Suçlar Sözleşmesi Ek Protokolü, Avrupa Anlaşma Serisi 189, 28.01.2003]
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS 198, 16.05.2005: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198>
[Suç Gelirlerinin Aklanması, Aranması, Zapt Edilmesi ve Müsaderesi Terörizmin Finansmanına İlişkin Sözleşme, Avrupa Konseyi Anlaşma Serisi 198, 16.05.2005]
- Convention on Laundering, Search, Seizure And Confiscation of the Proceeds From Crime, Strasbourg, ETS 141, 08.11.1990: <https://rm.coe.int/168007bd23>
[Suç Gelirlerinin Aklanması, Aranması, Zapt Edilmesi ve Müsaderesine İlişkin Sözleşme, Avrupa Anlaşma Serisi 141, 08.11.1990]
- MONEYVAL/Global Project on Cybercrime, Criminal money flows on the Internet - Typology research, March 2012: [http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL\(2013\)6_Reptyp_flows_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf)
[MONEYVAL/ Siber Suçlar, İnternet Üzerindeki Suç Kaynaklı Para Akışları Projesi – Tipoloji araştırması, Mart 2012]
- European Council Study on filtering, blocking and take-down of Illegal Content on the Internet, June 2016: <https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>
[İnternet Üzerindeki Yasadışı İçeriklerin Filtrelenmesi, Engellenmesi ve Kaldırılması Konulu Avrupa Konseyi Çalışması, Haziran 2016]
- Questionnaire on the use and efficiency of European Council instruments as regards international co-operation in the field of seizure and confiscation of proceeds of crime, including the management of confiscated goods and asset sharing. PC-OC Mod (2015) 06Rev4, 19.05.2016: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>
- [Müsadere edilmiş malların yönetimi ve varlık paylaşımı da dâhil olmak üzere, suç gelirlerinin zapt edilmesi ve müsaderesi alanındaki uluslararası işbirliği]

bakımından Avrupa Konseyi araçlarının kullanımı ve verimliliği konulu anket.
PC-OC Mod (2015) 06Rev4, 19.05.2016]

- Cybercrime Legislation – Country profiles:
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Document/s/CountryProfiles/default_en.asp
[Siber Suçlar Mevzuatı – Ülke profilleri]
- The functioning of 24/7 points of contact for cybercrime (discussion paper prepared by the Project on Cybercrime), April 2009:
<https://rm.coe.int/16802fa3be>
[Siber suçlar için 7/24 iletişim noktalarının işleyişi (Siber Suçlar Projesi tarafından hazırlanan müzakere dokümanı), Nisan 2009]
- Electronic Evidence Guide - A basic guide for police officers, prosecutors and judges(March 2013). Available subject to request at:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp
[Elektronik Kanıtlar Rehberi – Polis memurlarına, savcı ve hâkimlere yönelik temel bir rehber (Mart 2013). Talep üzerine şu bağlantıdan erişilebilir]
- T-CY(2006)04 – Strengthening co-operation between law enforcement and the private sector – examples of how the private sector has blocked child pornographic sites, 20 February 2006:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>
[T-CY(2006)04 – Kolluk kuvvetleri ile özel sektör arasındaki işbirliğinin kuvvetlendirilmesi – özel sektörün çocuk pornografisi sitelerini nasıl engellediğine ilişkin örnekler, 20 Şubat 2006]
- T-CY(2013)17rev - T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3 December 2014:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>
[T-CY(2013)17rev - Siber Suçlar Sözleşmesi Komitesi değerlendirme raporu: Budapeşte Siber Suçlar Sözleşmesi'nin hukuki yardımlaşma hükümleri, 3 Aralık 2014]
- T-CY(2014)17 - Rules on obtaining subscriber information report, December 2014:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1>
[T-CY(2014)17 - Abone bilgileri raporu elde edilmesine ilişkin kurallar, Aralık 2014]
- T-CY(2015)10 - Criminal justice access to data in the cloud: challenges, discussion paper prepared by the T-CY Cloud Evidence Group, May 2015:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>
[T-CY(2015)10 - Buluttaki verilere ceza yargılaması erişimi: güçlükler, Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu, Mayıs 2015]

- T-CY(2016)13 - Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers, T-CY Cloud Evidence Group, May 2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>
[T-CY(2016)13 - Hukuki yardımlaşma kanalları yoluyla ya da doğrudan hizmet sağlayıcılarına yapılan talepler yoluyla bir başka yargı yetkisi alanında depolanan verilerin derhal ifşa edilmesine yönelik fevkalade hal talepleri, Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu, Mayıs 2016]
- T-CY (2016)2 - Criminal justice access to data in the cloud: cooperation with "foreign" service providers. Background paper prepared by the T-CY Cloud Evidence Group, May 2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>
[T-CY (2016)2 - Buluttaki verilere ceza yargılaması erişimi: "yabancı" hizmet sağlayıcıları ile işbirliği. Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu tarafından hazırlanan arkaplan belgeleri, Mayıs 2016]
- T-CY(2016)7 - Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, final report of the T-CY Cloud Evidence Group, September 2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>
[T-CY(2016)7 - Buluttaki elektronik kanıtlara ceza yargılaması erişimi: Siber Suçlar Sözleşmesi Komitesi dikkatine sunulan tavsiyeler, Siber Suçlar Sözleşmesi Komitesi Bulut Kanıtları Grubu'nun nihai raporu, Eylül 2016]
- T-CY(2015)16 Adopted Guidance Note on Production Orders (Article 18) - Version 01 March 2017 (adopted by written procedure on 28 February 2017):
<https://rm.coe.int/16806f943e>
[T-CY(2015)16 Üretim Talimatlarına İlişkin Benimsenmiş Kılavuz Notu (Madde 18) - Versiyon 01 Mart 2017 (28 Şubat 2017 tarihinde yazılı prosedür ile kabul edilmiştir)]

7.2 Avrupa Birliği

- Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union OJ L 127/39, 29.4.2014
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042>
[Avrupa Birliği'nde suç vasıtaları ve gelirlerinin dondurulması ve müsadereesi hakkında, 3 Nisan 2014 tarihli, 2014/42/EU sayılı Avrupa Parlamentosu ve Avrupa Konseyi Direktifi, Resmi Gazete L 127/39, 29.4.2014]
- Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC:

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>

[Mali sistemin kara para aklama veya terörizmin finansmanı amaçlarıyla kullanılmasının önlenmesi hakkında, 20 Mayıs 2015 tarihli ve 2015/849 sayılı Avrupa Parlamentosu ve Avrupa Konseyi Direktifi, 648/2012 sayılı değişiklik getiren Avrupa Parlamentosu ve Avrupa Konseyi Yönetmeliği (AB), 2005/60/EC sayılı, iptal eden Avrupa Parlamentosu ve Avrupa Konseyi Direktifi ve 2006/70/EC sayılı Komisyon Direktifi]

- Joint Action 98/699/JHA of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime (OJ L 333, 9.12.1998, p. 1):

<http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=celex:31998F0699>

[Kara para aklama, suç vasıtaları ve gelirlerinin saptanması, izlenmesi, dondurulması, zapt edilmesi ve müsaderesi konulu, Avrupa Birliği Anlaşması Madde K.3 temelinde, Konsey tarafından benimsenen, 3 Aralık 1998 tarihli ve 98/699/JHA sayılı Ortak Eylem (Resmi Gazete L 333, 9.12.1998, s. 1)]

- Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (OJ L 182, 5.7.2001, p. 1):

<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>

[Kara para aklama, suç vasıtaları ve gelirlerinin saptanması, izlenmesi, dondurulması, zapt edilmesi ve müsaderesi konulu, 26 Haziran 2001 tarihli, 2001/500/JHA sayılı Konsey Çerçeve Kararı (Resmi Gazete 182, 5.7.2001, s. 1)]

- Council Framework Decision 2005/212/JHA of 24 February 2005 on confiscation of crime-related proceeds, instrumentalities and property (OJ L 68, 15.3.2005, p. 49):

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>

[Suç bağlantılı gelirler, vasıtalar ve mülklerin müsaderesi konulu, 24 Şubat 2005 tarihli, 2005/212/JHA sayılı Konsey Çerçeve Kararı (Resmi Gazete L 68, 15.3.2005, s. 49)]

- Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003):

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>
[content/EN/TXT/?uri=CELEX%3A32003F0577](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577)

[Malları veya kanıtları donduran emirlerin Avrupa Birliği'nde uygulanması hakkında, 22 Temmuz 2003 tarihli ve 2003/577/JHA sayılı Konsey Çerçeve Kararı (Resmi Gazete L 196, 2.8.2003)]

- Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (OJ L 328, 24.11.2006):

<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>

[Müsadere emirlerinin karşılıklı olarak tanınması ilkesinin uygulanması hakkında, 6 Ekim 2006 tarihli, 2006/783/JHA sayılı Konsey Çerçeve Kararı (Resmi Gazete L 328, 24.11.2006)]

- Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime (L 332/103, 18.12.2007):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>
[Suç gelirlerinin veya suçla ilişkili diğer mülklerin izlenmesi ve saptanması alanında Üye Devletlerin Varlık Geri Kazanımı Daireleri arasındaki işbirliğini konu alan, 6 Aralık 2007 tarihli, 2007/845/JHA sayılı Konsey Kararı (L 332/103, 18.12.2007)]
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA:
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>
[Bilgi sistemlerine karşı saldırıları konu alan, 12 Ağustos 2013 tarihli, 2013/40/EU sayılı Avrupa Parlamentosu ve Konsey Direktifi ve 2005/222/JHA sayılı, değiştiren Konsey Çerçeve Kararı]
- European Union Directive 2016/1148 on the security of network and information systems ("NIS Directive") of 6 July 2016:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG
[Ağ ve bilgi sistemleri güvenliği konulu, 6 Temmuz 2016 tarihli, 2016/1148 sayılı Avrupa Birliği Direktifi]
- EU GENVAL 2012 Final report on fifth round of mutual evaluation – "Financial crime and financial investigations":
<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>
[Karşılıklı değerlendirme beşinci raundu hakkında EU GENVAL 2012 nihai raporu –"Mali suçlar ve mali soruşturmalar"]
- Draft Final report of the seventh round of mutual evaluations on "The practical implementation an operation of the European policies on prevention and combating cybercrime", June 2017:
<http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>
["Pratik uygulama, siber suçların önlenmesi ve siber suçlarla mücadele alanındaki Avrupa politikalarının işleyişi" konulu, karşılıklı değerlendirmeler yedinci radundu nihai raporunun taslağı, Haziran 2017]

7.3 Birleşmiş Milletler

- United Nations Convention Against Illicit Traffic In Narcotic Drugs And Psychotropic Substances, Vienna, 19.12.1988:
<https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html>
[Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı Birleşmiş Milletler Sözleşmesi, Viyana, 19.12.1988]
- United Nations Convention Against Transnational Organized Crime, New York, 15.11.2000:
<https://www.unodc.org/unodc/en/treaties/CTOC/>

[Sınıraşan Organize Suçlara Karşı Birleşmiş Milletler Sözleşmesi, New York, 15.11.2000]

- United Nations Convention Against Corruption, New York, 31.10.2003:
<http://legal.un.org/avl/ha/uncc/uncc.html>
[Birleşmiş Milletler Yolsuzlukla Mücadele Sözleşmesi, New York, 31.10.2003]

7.4 Mali Eylem Görev Gücü

- International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, the FATF Recommendations, 2012:
<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>
[Kara Para Aklama, Terörizmin Finanse Edilmesi ve Silahlanma ile Mücadelede Uluslararası Standartlar, MEGG Tavsiyeleri, 2012]
- Money Laundering Using New Payment Methods, October 2010:
<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>
[Yeni Ödeme Yöntemleri Kullanarak Kara Para Aklama, Ekim 2010]
- Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014:
<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
[Sanal Para Birimleri Kilit Tanımlamaları ve Kara Para Aklama Karşısı Önlemler ve Terörizmin Finanse Edilmesi ile Mücadele Açısından Ortaya Çıkan Potansiyel Riskler, Haziran 2014]
- Virtual Currencies – Guidance for a risk-based approach, Financial Action Task Force, June 2015:
<http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
[Sanal Para Birimleri – Risk Temelli bir Yaklaşım için Kılavuz, Mali Eylem Görev Gücü, Haziran 2015]

7.5 İçtihat

- European Court of Human Rights (ECtHR) Judgement in K.U. v. Finland, 2 December 2008, on the obligation of Governments to protect individuals against crime, including through criminal law:
<http://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22K.U.%20v.%20Finland%22%5D,%22documentcollectionid%22:%5B%22GRANDCHAMBER%22,%22CHAMBER%22%5D,%22itemid%22:%5B%22001-89964%22%5D%7D>
[K.U. ile Finlandiya arasındaki davada, ceza hukuku yolu da dahil olmak üzere, devletlerin bireyleri suça karşı koruma yükümlülüğü ile ilgili, 2 Aralık 2008 tarihli Avrupa İnsan Hakları Mahkemesi (AİHM) Kararı]
- ECtHR case law on Personal Data Protection:
http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
[Kişisel Verilerin Korunması ile ilgili AİHM içtihadı]

- ECtHR case law on New Technologies:
http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf
[Yeni Teknolojiler ile ilgili AİHM içtihadı]
- ECtHR case law on Mass Surveillance:
http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
[Kitleli Gözetleme ile ilgili AİHM içtihadı]
- Court of Justice of the European Union Judgement in Joined Cases C-293/12 and C-594/12. Digital Rights Ireland and Seitlinger and Others:
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
[Birlikte Görülen C-293/12 ve C-594/12 Davalarında Avrupa Birliği Adalet Mahkemesi Kararı. Digital Rights Ireland ile Seitlinger ve Diğerleri]
- EU Court of Justice of the European Union Judgement in Case C-582/14, 19 October 2016, dynamic IP addresses may qualify as 'personal data' under EU privacy law:
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1034974>
[Avrupa Birliği AB Adalet Mahkemesi]
- Court of Justice of the European Union Judgement in Case C-264/14, 22 October 2015, "‘bitcoin’ virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators":
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=160800>
[Avrupa Birliği Adalet Mahkemesi]
- Supreme Court of Belgium ruling in the case of Belgium vs. Yahoo!: http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1
[Belçika ile Yahoo! Arasındaki davada Belçika Yüksek Mahkemesi hükmü]
- US Court of Appeals ruling in the case of Microsoft vs. United States: <http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412>
[Microsoft ile Birleşik Devletler arasındaki davada ABD Temyiz Mahkemesi hükmü]

7.6 Diğer referanslar

- Data Retention after the Judgement of the Court of Justice of the European Union, Prof. Dr. Franziska Boehm et al., Munster/Luxembourg, 30 June 2014:
http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf
[Avrupa Birliği Adalet Mahkemesi'nin Kararı sonrasında Verilerin Saklanması, Prof. Dr. Franziska Boehm ve diğ., Munster/Lüksemburg, 30 Haziran 2014]
- Encryption a Matter of Human Rights, Amnesty International Report, March 2016. Available at:

http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

[Bir İnsan Hakları Meselesi olarak Şifreleme, Uluslararası Af Örgütü Raporu, Mart 2016. Ulaşmak için bkz.]

- "Brochure: The 6 need-to-knows about Financial Investigation", February 2016:
<https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>
["Broşür: Finansal Soruşturma Hakkında Bilinmesi Gereken 6 Şey", Şubat 2016]
- "Needs assessment on tools and methods of financial investigation in the European Union", ECORYS, Aralık 2015:
https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf
["Avrupa Birliği'nde mali soruşturma araçları ve yöntemleri ihtiyaç değerlendirmesi", ECORYS, Aralık 2015]
- European Banking Authority Opinion on 'virtual currencies', EBA/Op/2014/08, July 2014:
<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>
["Sanal para birimleri" ile ilgili Avrupa Bankacılık Otoritesi Görüşü, EBA/Op/2014/08, Temmuz 2014]
- An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, Koshy *et al*, Pennsylvania State University:
http://fc14.ifca.ai/papers/fc14_submission_71.pdf
[P2P Ağ Trafiği Kullanan Bitcoında Anonimlik Analizi, Koshy ve diğ., Pennsylvania Eyalet Üniversitesi]
- The Internet Organised Crime Threat Assessment (IOCTA) 2016, Europol:
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>
[Organize İnternet Suçları Tehdidi Değerlendirmesi (IOCTA) 2016, Europol]
- The Internet Organised Crime Threat Assessment (IOCTA) 2017, Europol:
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>
[Organize İnternet Suçları Tehdidi Değerlendirmesi (IOCTA) 2017, Europol]