This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

SİBER SUÇLARIN ÖNLENMESİ VE BU SUÇLARLA MÜCADELE: TÜRKİYE İÇİN TEMEL BULGULAR VE TAVSİYELER

Türkiye'de Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması

Avrupa Birliği – Avrupa Konseyi Ortak Projesi

This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

SİBER SUÇLARIN ÖNLENMESİ VE BU SUÇLARLA MÜCADELE: TÜRKİYE İÇİN TEMEL BULGULAR VE TAVSİYELER

Türkiye'de Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması

Avrupa Birliği – Avrupa Konseyi Ortak Projesi

SİBER SUÇLARIN ÖNLENMESİ VE BU SUÇLARLA MÜCADELE: TÜRKİYE İÇİN TEMEL BULGULAR VE TAVSİYELER

Hazırlayan
- Esther George
- Dr. Michael Jameison
- Kemal Kumkumoğlu

Bu Rapor "Türkiye'de Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması" Avrupa Birliği ve Avrupa Konseyi Ortak Projesi kapsamında hazırlanmıştır. Bu Proje Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmekte, Avrupa Konseyi tarafından yürütülmektedir. Projenin yararlanıcı kurumları Türkiye Cumhuriyeti Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü ve Türkiye Adalet Akademisidir. Projenin sözleşme makamı Merkezi Finans ve İhale Birimidir.

Bu Rapor, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmiştir. Burada ifade edilen görüşler hiçbir şekilde tarafların resmi görüşünü yansıtmamaktadır. Bu Raporda yer alan görüş ve düşünceler yazarın sorumluluğundadır.

Tasarım
Bilge Bostan

Baskı
Tam Pozitif Reklamcılık | Matbaa
Çamlıca Mahallesi Anadolu Bulvarı
145. Sokak 10/11
Yenimahalle/ANKARA
Tel: 0312 397 00 31 | Faks: 0312 397 86 12
E-Posta: pozitif@pozitifmatbaa.com

Proje Paydaşları
- Anayasa Mahkemesi
- Yargıtay Başkanlığı
- Hâkimler ve Savcılar Kurulu
- Türkiye Barolar Birliği
- Mali Suçlar Araştırma Kurulu Başkanlığı (MASAK)
- Jandarma Genel Komutanlığı
- Emniyet Genel Müdürlüğü
  - Siber Suçlarla Mücadele Daire Başkanlığı
  - Terörle Mücadele Daire Başkanlığı
  - Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı
- Bilgi Teknolojileri ve İletişim Kurumu
- Adli Tıp Kurumu

www.coe.int/tr/web/ankara
Avrupa Konseyi Ankara Program Ofisi

cas.ankara@coe.int
Ceza Adalet Sisteminin Güçlendirilmesi Projesi
cas_projesi
@project_cas
Ceza Adalet Sisteminin Güçlendirilmesi Projesi

İÇİNDEKİLER

YÖNETİCİ ÖZETİ

Bağlam

Siber suçlar bugün dünyada en hızlı büyüyen suçlar arasındadır. Sessiz ve yıkıcı olan bu suçlar bireyleri, şirketleri ve devlet altyapılarını etkiler. Sadece finansal dolandırıcılık ve veri kaybıyla ilgili değil, aynı zamanda siber zorbalık, kişisel verilerin kaybı gibi hedefe yönelik suç faaliyetleriyle de ilgilidirler. Siber suçlar sınırlar ötesinde işlendiği için herhangi bir ülkeyle sınırlı değildir; bu nedenle iş birliğine ve ortak uluslararası ve ulusal stratejilere her zamankinden daha fazla ihtiyaç duyulmaktadır.

Siber suçlar da dâhil olmak üzere Türkiye'nin ceza adaleti alanında karşılaştığı zorlukları tespit etmek amacıyla Avrupa Konseyi, Türk yargısının ceza adaleti alanında uluslararası standartlara ve Avrupa standartlarına uygunluğunu sağlayarak daha etkin, etkili ve görünür hale getirilmesini ve güçlendirilmesini amaçlayan bir Avrupa Birliği - Avrupa Konseyi programı olan 'Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması Ortak Projesinin' (Ortak Proje) başlangıcında bir İhtiyaç Analizi yapılmasını sağlamıştır.

İhtiyaç analizi sonrasında hazırlanan İhtiyaç Değerlendirme Raporunda sunulan önemli tavsiyeler, siber suçların soruşturulması ve kovuşturulmasında görev alan makamlar arasındaki koordinasyonun daha da güçlendirilmesi ihtiyacı ve özellikle aşağıdaki ihtiyaçlarla ilgilidir:

- Siber suçlarla ilgilenen Emniyet Genel Müdürlüğü ve Jandarma birimlerinin bu alandaki deneyimlerini paylaşmaya teşvik edilmesi (bölüm 266);

- Ülke içindeki farklı yargı çevrelerinde siber suçların soruşturulması için merkezi bir dosyalama sisteminin kurulmasının değerlendirilmesi (bölüm 268);

- Cumhuriyet savcılıkları bünyesinde sadece siber suç davalarıyla ilgilenmek üzere özel savcılık bölümleri veya birimleri kurulmasının değerlendirilmesi (bölüm 274);

• Adalet Bakanlığından savcılara uluslararası istinabe talepleri de dâhil olmak üzere, birimler arasında daha hızlı iletişim sağlamaya yönelik kılavuzların ve şablonların uygulanması (bölüm 291).

Bu doğrultuda, karşılaşılan zorlukları değerlendirmek ve siber suçların soruşturulması ve kovuşturulmasında yetkili makamlar arasında daha iyi koordinasyon ve iş birliğinin nasıl sağlanabileceğini ve/veya geliştirilebileceğini belirlemek amacıyla Türkiye Adalet Bakanlığı ortaklığında sekiz koordinasyon toplantısı düzenlenmiştir. Etkinlikler aşağıdaki tarihlerde aşağıda belirtilen yerlerde gerçekleştirilmiştir:

• Ankara - 25-26 Ekim 2021,
• İstanbul - 16-17 Aralık 2021,
• İzmir - 10-11 Şubat 2022,
• Adana - 24-25 Şubat 2022,
• Antalya - 17-18 Mart 2022,
• Samsun - 7-8 Eylül 2022,
• Diyarbakır - 23-24 Kasım 2022,
• Konya - 10-11 Ocak 2023.

Bu raporda, Ortak Proje kapsamında düzenlenen sekiz koordinasyon toplantısında kolluk kuvvetleri, adli bilişim uzmanları, bilgi teknolojisi uzmanları, savcılar, yargı mensupları ve bankacılık sektörü temsilcileri tarafından oluşturulan temel tavsiyeleri gözden geçirmek ve özetlemek amacıyla yazarlar Esther George (Birleşik Krallık'ta eski Savcı), Kemal Kumkumoğlu (Türkiye'de Avukat) ve Mick Jameison (Birleşik Krallık'ta eski Kolluk Görevlisi) tarafından hazırlanan politika özetleri bir araya getirilmiştir. Diğer materyal kaynakları Dr. Burcu Baytemir Kontacı'nın notlarıdır.

Bu raporun, Türkiye'nin siber suçlarla mücadele için kapsayıcı bir strateji geliştirmesinde ilk adım olarak kullanılabileceği umulmaktadır. Bu strateji, uygulama için farklı aşamaların belirlenmesi ve uygun kaynakların sağlanması gereken uzun vadeli bir strateji olarak görülmektedir. Siber suçlarla mücadele, eğitim, iş birliği (ulusal, bölgesel ve uluslararası), bilgi alışverişi, kamuoyu farkındalığı, raporlama, uygun mevzuat ve caydırıcı cezalar gibi çok çeşitli müdahaleleri gerektirmektedir. Türkiye, Avrupa Konseyi Siber Suç Sözleşmesini ('Budapeşte Sözleşmesi') imzalamış olduğundan, siber suçlarla tüm unsurlarıyla mücadele etmek için dinamik ve sürdürülebilir bir strateji geliştirilmesine yardımcı olacak kapasite geliştirme kaynaklarına erişime sahiptir.

A. ARKA PLAN

Bulgular

Siber suçlarla mücadelenin önündeki en başlıca engel, bu dijital suçların arkasındaki suçluların tespit edilmesi ve yakalanmasıdır. Siber suçlular sıklıkla farklı yargı bölgelerinde faaliyet göstermekte ve takip edilmekten kaçınmak için genellikle anonimlik veya sahte anonimlikten yararlanmaktadır. Ayrıca, uluslararası soruşturmaların yürütülmesinde ve iş birliğinin geliştirilmesinde önemli engeller bulunmaktadır. Bir diğer önemli sorun da siber suç olaylarının hem bireyler hem de büyük şirketler tarafından eksik bildirilmesidir. Fidye yazılımı vakalarına bakıldığında, 'fidye' genellikle daha fazla sorundan ve kişisel verilerim güvenliğini sağlama konusunda şirkete duyulan güven kaybı gibi yansımalardan kaçınmak için ödenir.

Hızla değişen teknoloji ortamı nedeniyle kolluk kuvvetleri tarafından kullanılan yöntemlerin çoğu zaman etkisiz kaldığı kabul edilmektedir. Bu durum, bankalar ve hatta adli bilişim departmanları gibi dış kurumların zamanında iş birliği yapmaması nedeniyle aksamaktadır. Ayrıca, siber suçlular suç faaliyetlerini kolaylaştırmak için en yeni teknolojilere başvurabilirken, kolluk kuvvetleri kaynak ve eğitim açısından teknolojinin gelişimine ayak uydurmakta zorlanmaktadır.

Savcılığın ve Yargının bu alanda teknik karmaşıklık, hacim ve karmaşıklık bakımından artmaya devam eden siber suçlar ve elektronik delillerle ilgili yüksek iş yükü gibi pek çok zorlukla karşı karşıya olduğu tespit edilmiştir. Özel işletmelerin, bankaların ve hizmet sağlayıcıların bilgi taleplerine zamanında cevap vermemeleri, davalar üzerinde zincirleme olarak olumsuz bir etki yaratarak aşırı bir başarısızlık oluşturmuştur.

Adli bilişimin karşılaştığı zorluklara ilişkin olarak yapılan bir değerlendirmede, iş yükünün, yani analiz gerektiren cihazların sayısının (incelemenin kalitesinden ziyade) ve savcıların teknik konuları anlamaması nedeniyle adli bilişim incelemecilerinin doğru bir şekilde yönlendirilememesinin önemli sorunlar olduğu görülmüştür. Delillerin teslimi ve delillerin taşınmasının, nasıl ele alındıkları ve laboratuvara gönderildikleri konusunda sorun bulunmaktadır.

Seçilen tavsiyeler

Sekiz koordinasyon toplantısının sonucunda, bu raporun sonuç bölümünde de detaylandırıldığı üzere, birçok tavsiye ortaya çıkmıştır. En önemli tavsiyeler aşağıda verilmiştir:

• Ulusal Siber Suç Biriminin (USSB) oluşturulması.

• Siber suç soruşturmalarında ve elektronik delillerin ele alınması ve sunulmasında en iyi uygulamaların teşvik edilmesi.

• Çocuklara yönelik çevrim içi istismarla mücadele alanında görevli bir birimin oluşturulması.

• Siber suçlar için çevrim içi bir ulusal raporlama merkezinin oluşturulması.

• Kolluk kuvvetleri tarafından personeli elde tutma planları da dâhil olmak üzere bütüncül bir eğitim stratejisinin uygulanması.

• Çözülme olasılığı düşük olan ya da soruşturulmaya değmeyecek kadar az mali kayıp yaratan suçların elenerek soruşturulmaması için savcılık birimleri ve polis arasında bir iş birliği anlaşması yoluyla bir eleme sisteminin oluşturulması.

• Kurumlar Arası İş Birliği Protokolü başlıklı iPROCEEDS belgesinin tavsiyelerinin uygulanması.

• Okullarda ve halka yönelik olarak suç önleme ve farkındalık kampanyalarının düzenlenmesi.

• Ulusal ve yerel düzeyde siber suçların önlenmesi için özel birimlerin oluşturulması.

• 7/24 Tek İrtibat Noktasının rolü hakkındaki bilgilerin ve irtibat noktasına ulaşma yollarının paylaşılmasına ilişkin bilgilerin yaygınlaştırılması.

• Hâkimlere, savcılara ve kolluk kuvvetlerine uzmanlık eğitimi verilmesi.

• Siber suç mağdurlarına destek ve kaynak sağlanmasına yönelik bir strateji geliştirilmesi.

• Elektronik delillerin toplanması ve yargılama yetkisi ile ilgili cezai usul hükümleri gibi mevzuattaki eksikliklerin ele alınması.

• Çocukların İnternette kandırılarak istismar edilmesi ve fidye yazılımları gibi yeni suç türlerinin belirlenmesi.

• Kapsayıcı bir siber güvenlik mevzuatının düzenlenmesi ve kolluk kuvvetlerinin faaliyetlerine ilişkin veri koruma hükümlerinde reform yapılması.

• Budapeşte Sözleşmesinin 2. Protokolünün iç hukuka aktarılması.

1. Paydaşlar ve Diğer Bilgiler

Sekiz ilde gerçekleştirilen toplantılara çeşitli kurumlardan temsilciler katılmıştır. Bunlar sırasıyla şunlardır:

Adli Makamlardan Temsilciler,
• İlk Derece Mahkemesi Hâkimleri
• Bölge Adliye Mahkemeleri
• Bölge İdare Mahkemeleri
• Cumhuriyet Savcıları

Kamu Kurumlarından Temsilciler,
• Bankacılık Düzenleme ve Denetleme Kurumu
• Adli Tıp Kurumu
• Bilgi Teknolojileri ve İletişim Kurumu,

• MASAK (Mali Suçlar Araştırma Kurulu)
• Adalet Bakanlığı

Barolardan Temsilciler,
• İzmir Barosu
• Adana Barosu
• Antalya Barosu
• Samsun Barosu
• Türkiye Barolar Birliği

Emniyet Müdürlüğü ve İl Jandarma Komutanlığı Temsilcileri,
• Adana İl Emniyet Müdürlüğü
• Antalya İl Emniyet Müdürlüğü,
• Antalya İl Jandarma Komutanlığı,
• Diyarbakır İl Emniyet Müdürlüğü,
• Diyarbakır İl Jandarma Komutanlığı
• Konya İl Emniyet Müdürlüğü,
• Konya İl Jandarma Komutanlığı,
• Samsun İl Emniyet Müdürlüğü,
• Samsun İl Jandarma Komutanlığı

Diğer Derneklerden Temsilciler,
• Türk Ceza Hukuku Derneği
• Adli Bilişim ve Bilişim Hukuku Derneği
• Türkiye Bankalar Birliği
• Uluslararası Çocuk Merkezi ve Çocuk Hakları Merkezi
• Bilişim Hukuku Derneği

B. BULGULAR

1. Türkiye'de Siber Suçların Etkisi

a. Büyüyen siber suç tehdidine kısa bir genel bakış

Dünya İnternet aracılığıyla birbirine daha bağlı hale geldikçe, siber suçlar hem bireyler hem de kuruluşlar için büyük bir endişe kaynağı haline gelmektedir.

Siber suçlar sadece bireyler için değil, aynı zamanda tüm ülkeler ve sektörlerdeki her şekil ve büyüklükte işletmeler ve devlet kurumları için de büyüyen bir tehdit olmaya devam etmektedir. Dünyada en hızlı büyüyen suçlardır ve kurumlar ve bireyler eskisinden çok daha fazla siber saldırıyla karşı karşıyadır. Suçlular faaliyetlerini giderek daha fazla İnternete taşımaktadır çünkü İnternet paranın bulunduğu yerdir. Siber suçların neden cazip olduğunu anlamak kolaydır, zira siber suçlar esasen düşük riskli ve son derece büyük getirileri olan suçlardır. Siber suçlular yakalanma korkusu olmadan büyük mali kazançlar elde edebilirler. Bunun nedeni kısmen şirketlerin fidye yazılımları gibi siber suçları kamuoyundaki yankıları ve itibar riski nedeniyle bildirme konusundaki

isteksizliğidir. Ayrıca suçlular küresel ağlarda çalışma konusunda giderek daha becerikli hale gelmekte, kendilerine yardımcı olacak teknolojilere erişebilmekte ve bunları geliştirebilmektedir. Ayrıca, siber suçluların güvenli ve sözde anonim ödeme sistemlerine erişimleri olduğundan, onları yakalamak çok daha zor hale gelmektedir.

Siber suç ve siber ortam destekli suç kavramlarının her ikisi de teknoloji içeren suçların alt kümeleridir, ancak ikisi arasında önemli farklar vardır.

Siber suç, doğrudan bilgisayarlara ve bilgisayar ağlarına karşı işlenen suçları ifade eder. Bu tür suçlar yalnızca bilgi teknolojileri kullanılarak işlenebilir.

Örnekleri arasında kötü amaçlı yazılımlarının yayılması, ağlara, bilgisayarlara, programlara veya verilere karşı işlenen suçlar, bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı işlenen suçlar yer almaktadır.

Öte yandan, siber ortam destekli suçlar, bilgisayarın geleneksel suç faaliyetlerini kolaylaştırmak için bir araç olarak hizmet ettiği durumları içerir. Örneğin, bilgisayarlardan önce işlenen bir suç olan dolandırıcılık, dijital teknoloji kullanılarak işlendiğinde bu kategoriye girer. Bu kategori aynı zamanda fikri mülkiyet hakları ve benzeri haklarla bağlantılı suçların yanı sıra bilgisayarla bağlantılı sahtecilik ve çocukların cinsel istismarına yönelik materyallerin dağıtımı gibi geleneksel suçların işlenmesinde İnternetin kullanılmasını da kapsamaktadır.

Türkiye'de artan siber suç tehdidi hem bireyler hem de işletmeler için büyük bir endişe kaynağıdır. Bu alanda incelenebilecek alt konulardan biri, ülkede yaygın olan farklı siber suç türleridir. Kimlik avı, fidye yazılımı saldırıları, kimlik hırsızlığı ve veri ihlalleri Türkiye'de karşılaşılan en yaygın siber suç türlerinden bazılarıdır.

Kimlik avı, kullanıcı adları, şifreler ve kredi kartı bilgileri gibi hassas bilgileri elde etmeye yönelik hileli girişimleri içerir. Bu tür siber suçlar genellikle sahte e-postalar veya meşru gibi görünen İnternet sitelerinin kullanımıyla gerçekleşir.

Fidye yazılımı saldırıları, son yıllarda giderek yaygınlaşan başka bir siber suç türüdür. Bu saldırılar, kurbanın dosyalarını ve bilgisayar sabit disklerini şifreleyen ve bunların şifresinin çözülmesi karşılığında ödeme talep eden kötü amaçlı yazılımların kullanımını içerir.

Kimlik hırsızlığı da Türkiye'nin siber uzayında önemli bir sorundur. Suçlular çalıntı kişisel bilgileri kullanarak mağdurların bilgisi dışında banka hesabı açabilir veya alışveriş yapabilirler.

Son olarak, kuruluşlar tarafından saklanan hassas bilgilere yetkisiz kişiler tarafından erişildiğinde veri ihlalleri meydana gelebilir. Bu durum işletmeler için mali kayıplara yol açabilir ve bireylerin mahremiyeti için risk oluşturabilir.

Siber saldırılar şirketlere mali kayıplar yaşatarak ekonomiyi etkilemektedir. Veri ihlalleri nedeniyle şirketler itibarını ve müşterilerinin güvenini kaybedebileceğinden, siber suçların işletmeler üzerindeki etkisi ciddi olabilir. Siber saldırıların yol açtığı zarar çok büyük olabilir, önemli mali kayıplara ve hatta

bazı durumlarda iflasa sebebiyet verebilir. Siber suçlular yöntemlerini sürekli olarak geliştirmektedir, bu durum ise şirketlerin kendilerini bu saldırılardan korumalarını giderek zorlaştırmaktadır. Başarılı bir siber saldırı hassas verilerin, fikri mülkiyetin ve finansal bilgilerin kaybına neden olabileceğinden, işletmeler ve devlet kurumları daha ciddi sonuçlarla karşı karşıya kalmaktadır. Bu tür saldırılarla ilişkili maliyetler astronomik düzeyde olabilir ve kurumun etkin bir şekilde faaliyet gösterme imkânları üzerinde uzun süreli etkilere sahip olabilir. Ayrıca, müşterilerin ve paydaşların güveninin kaybedilmesine yol açabilir ve bu güvenin yeniden kazanılması yıllar alabilir.

Tüm suçlular gibi siber suçlular da birbirleriyle iletişim kurmaya ve birbirlerinden bir şeyler öğrenmeye çalışırlar. Suç forumları ve pazarları, grup sohbetleri ve hatta Facebook sayfaları bu yeraltı ekonomisi için üreme alanları olarak hizmet vermekte ve tehdit aktörlerinin stratejilerini kendi özel bağlamlarına ve dünyanın her yerindeki hedeflerine uyarlamalarına olanak sağlamaktadır. Örneğin, Birleşik Krallık'taki COVID salgını sırasında dolandırıcılar vergi dolandırıcılığı yapmak için kişisel vergi hesaplarını ele geçirmeye çalışmışlardır.

Mobil cihazların artan kullanımı, akıllı telefon kullanıcılarını hedef alan kötü amaçlı uygulamalar ve kimlik avı saldırıları da dâhil olmak üzere mobil teknoloji bağlantılı siber suçlarda da bir artışa yol açmıştır. Bu eğilimlerin de gösterdiği gibi, siber suç tehdidi sürekli olarak geliştiğinden ve daha karmaşık bir hal aldığından, hem bireylerin hem de kurumların olası tehditlere karşı tetikte olmaları gerekmektedir.

b. Siber suçlarla mücadele için etkili bir strateji geliştirmenin önemi

Türkiye'de *siber güvenlik* olayları USOM tarafından raporlanmakta ve ele alınmakta olup rutin olarak kolluk kuvvetlerine intikal ettirilmemektedir. Siber güvenlik olayları, bir kuruluşun sistemlerinin veya verilerinin tehlikeye girdiğini veya bunları korumak için alınan önlemlerin başarısız olduğunu gösterebilecek olaylardır. Olay bildirimleri tipik olarak bir siber güvenlik taksonomisine göre sınıflandırılır. USOM'nin rolü ve Türkiye'de siber güvenlikle mücadelesi Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) ile güçlendirilmiştir.[1]

Siber suç konuları, ulusal yasal çerçeveye aykırı olan suç faaliyetleridir ve bu raporlama sistemleri buna göre sınıflandırılmıştır. Siber suçlar için tam raporlama ve soruşturma mekanizmaları genellikle savcılar ve kolluk kuvvetleri tarafından yönetilmektedir. Ulusal Güvenlik Stratejisi ve Eylem Planında siber suçlarla ilgili sınırlı yorum yer almakta ve kapasite geliştirme, uluslararası bilgi paylaşımı ve uluslararası ortaklıkların önemli olduğu belirtilmektedir. Bunlar dışında, siber suçlarla mücadele için eylem planlarının uygulamaya koyulmasına yönelik sınırlı hususlar bulunmaktadır.

[1] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf

Özellikle yeni teknolojiler ortaya çıktıkça ve geliştikçe katlanarak büyüyen suçlar olan siber suçlarla mücadele için Türkiye'nin kapsayıcı ve etkili bir strateji (ulusal, bölgesel ve uluslararası boyutları kapsayan) geliştirmesi ve uygulaması zorunludur. Siber suçlar oldukça karmaşıktır, yenilikçi taktikler kullanılarak güvenlik açıklarından faydalanılmasına dayanır ve bu durumun kısa ve orta vadede iyileşmesi beklenmemektedir. İçinde bulunduğumuz bu dijital çağda, kişisel verilerimizden hayatımızı nasıl sürdürdüğümüze kadar her şey sosyal medyada siber suçluların istismarına açık durumdadır.

Siber suçlarla mücadelede karşılaşılan en büyük zorluk, siber uzayda suç işleyenlerin izini sürmek ve onları yakalamaktır. Siber suçlar rapor edildiğinde, kolluk kuvvetlerinin soruşturma yapmak için kullandığı geleneksel yöntemler, gelişen dijital ortamda genellikle etkisiz kalmakta ve siber suçluların adalete teslim edilmesini zorlaştırmaktadır. Bu sorunla mücadele etmek için, kolluk kuvvetleri, siber suç işleyenleri takip etmeye ve kovuşturmaya yardımcı olacak yeni stratejiler, taktikler ve araçlar benimsemelidir ve benimsemektedir.

Bu stratejilerden biri, polis departmanlarında yalnızca siber suçları soruşturmaya odaklanan uzman birimlerin oluşturulmasıdır. Bu birimlerde adli bilişim ve diğer ilgili alanlarda uzmanlık eğitimi almış memurlar çalışmaktadır.

Başka bir strateji de kolluk kuvvetleri arasında uluslararası iş birliğinin artırılmasıdır. Siber suçlar sınır tanımadığından, ülkelerin kendi yetki alanları dışında faaliyet gösteren suçluların izini sürmek için birlikte çalışmaları çok önemlidir. Kolluk kuvvetleri arasında sınır ötesi iş birliği ve bilgi paylaşımı, etkili siber suç stratejilerinin kritik bir unsurudur.

Bunun uluslararası örneklerinden biri, istihbarat paylaşmak, operasyonları koordine etmek ve siber suçluları hedef almak üzere Avrupa'nın dört bir yanından kolluk kuvvetlerini bir araya getiren Avrupa Birliği'nin "Ortak Siber Suç Eylem Görev Gücü" (J-CAT) adlı oluşumdur. J-CAT, çevrim içi dolandırıcılık, kötü amaçlı yazılımların dağıtımı ve bilgisayar korsanlığı gibi faaliyetlerde bulunan çok sayıda suç şebekesini çökertmede başarılı olmuştur.

Başka bir örnek de Avustralya, Kanada, Yeni Zelanda, Birleşik Krallık ve Amerika Birleşik Devletleri arasında siber tehditlere ilişkin istihbarat paylaşımına ve üye ülkelerin soruşturma ve kovuşturmalarda iş birliği yapmasına olanak tanıyan "Beş Göz" ittifakıdır.

Uluslararası Kriminal Polis Teşkilatı (INTERPOL) da siber suçlar konusunda sınır ötesi iş birliğinin kolaylaştırılmasında önemli bir rol oynamaktadır. INTERPOL, Küresel İnovasyon Kompleksi (IGCI) aracılığıyla dünyanın dört bir yanındaki kolluk kuvvetlerine eğitim ve destek sağlamakta ve karmaşık siber suçlara yönelik ortak soruşturmaların yürütülmesini kolaylaştırmaktadır.

Türkiye, Avrupa Konseyi Siber Suç Sözleşmesini (Budapeşte Sözleşmesi) onayladığından, siber suçlarla mücadele yaklaşımını güçlendirecek kapasite geliştirme, uluslararası iş birliği ve usul hukuku araçlarına erişim sahibidir.

Türkiye, sınır ötesi hizmet sağlayıcılarla doğrudan iş birliği veya acil durumlarda iş birliği gibi gelişmiş iş birliği ve elektronik delillerin ifşasına ilişkin ek ve hızlandırılmış araçlar sağlayan Budapeşte Sözleşmesinin İkinci Ek Protokolünü imzalamayı ve onaylamayı değerlendirmelidir.

Kolluk kuvvetleri arasında sınır ötesi iş birliği ve bilgi paylaşımı, etkili siber suç stratejilerinin temel bileşenleridir. Kamu-özel sektör ortaklıkları ve iş birliği, dünyanın çeşitli ülkelerinde etkili siber suç stratejilerinin temel bileşenleri olarak tanımlanmaktadır.

Türkiye genelinde düzenlenen sekiz çalıştayda, siber suçlarla mücadele çalışmalarının ulusal, bölgesel ve uluslararası düzeyde bir 'ekip çalışması' olması gerektiği vurgulanmıştır. Bu çalışmalar, ulusal, bölgesel ve uluslararası kurumlar arasında iş birliğini, eğitim faaliyetlerini (her alanda), bankalar, müfettişler ve savcılar arasında karşılıklı yardımlaşmayı, halkın bilinçlendirilmesini, riskler ve uygunluğu, siber etiği, okullarda ebeveynlerin, bakıcıların ve çocukların eğitimini, raporlamayı ve toplanan delillerin nitelikli olmasının sağlanmasını içerir.

Bu alanları kapsayan, iyi tasarlanmış, uzun vadeli ve kapsayıcı bir strateji Türkiye'ye siber suçlarla mücadelede yardımcı olacaktır. Bu strateji, uygulama aşamaları ve sürekli gözden geçirmeyi içeren donanımlı bir strateji olmalıdır. Gelişen teknolojilere ve bunlara karşı koyma yollarına ayak uydurmalıdır.

2. Mevzuat

Siber suçlara ilişkin mevcut hukuki çerçevedeki eksiklikler ve bunlardan kaynaklanan zorluklar çalıştay katılımcıları tarafından geniş ölçüde kabul görmüştür. Ulusal ve uluslararası mevzuat birlikte değerlendirildiğinde, siber suçlarla mücadelede esas alınabilecek temel hükümler Türk Ceza Kanunundaki siber suçlarla ilgili hükümlerdir. Bunlar aşağıdaki gibi suçları içermektedir:

• Bilişim Sistemine Girme (Madde 243),

• Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (Madde 244),

• Banka veya Kredi Kartlarının Kötüye Kullanılması (Madde 245), Yasaklanmış Cihaz veya Programlar(ın Kullanılması) (Madde 245/a),

• İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (Kanun No. 5651),

• Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun),

• Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte Sözleşmesi) siber suçlara ilişkin hükümler içermektedir.

Çalıştaylarda hem kolluk kuvvetleri personelinin hem de hâkim ve savcıların siber suçlara ilişkin mevcut hukuki çerçeveye yeterince aşina olmadıkları tartışılmıştır. Bu durum, teknik konular hakkında anlayış eksikliği ile birlikte, siber suçlarla ilgili yasa ve yönetmeliklerin bazı durumlarda uygulanmamasının nedenlerinden bazılarını açıklamaktadır. Birçok yetkili, bu konulardaki genel bilgi eksikliklerini ve mevcut durumdan duydukları memnuniyetsizliği dile getirmiştir.

Prensip olarak, soruşturma ve kovuşturmalar genellikle sadece Türk Ceza Kanunu ve Ceza Muhakemeleri Usulü Kanunu çerçevesinde yürütülmektedir. Çalıştaylar sırasında birçok kolluk kuvveti personeli ve birçok hâkim ve savcının Budapeşte Siber Suçlar Sözleşmesinden haberdar bile olmadığı görülmüştür. Ayrıca, karşılaştıkları ihbar ve şikâyetlere dair soruşturmalarında güvenebilecekleri bir kaynağa sahip olmadıklarını belirtmişlerdir.

Ayrıca, geleneksel suçların neredeyse tamamının bilişim teknolojileri aracılığıyla işlenebiliyor olması, uzman kolluk görevlilerinin, hâkimlerin ve savcıların iş yükünü artırmaktadır. Soruşturma ve kovuşturma aşamalarında, özellikle delillerin toplanması ve değerlendirilmesinde siber suçlara ilişkin özel usullerin uygulanmasını gerektirmektedir. Siber suçlara ilişkin yürütülen soruşturmalar açısından bu özel usullerde kilit noktanın "hız" olduğu görülmektedir. Bu konuda özel bir örnek, dolandırıcılık suçunun nitelikli hali olarak düzenlenen "Bilişim sistemleri, banka veya kredi kurumlarının kullanılması suretiyle işlenen dolandırıcılık" suçudur. Gerçekten de geleneksel bir suç olan dolandırıcılık suçu bu şekilde siber suç haline dönüşmektedir. Failin tespitinden delillerin toplanmasına kadar geçen sürede neredeyse tüm deliller kaybolma riski taşıyabilmektedir.

Siber suçlara ilişkin başlıca (hukuki) sorunlar arasında, siber suçlara ilişkin kapsamlı ve açıklayıcı bağımsız bir düzenlemenin olmaması, yürürlükteki mevzuatın yetersizliği, neredeyse tüm suçların artık bilişim teknolojileri aracılığıyla işlenebiliyor olması, suçun işlendiği yerin tespit edilememesi ve buna bağlı olarak adli makamlar arasında ortaya çıkan yetki uyuşmazlıkları, elektronik delillere zaman içerisinde ulaşmanın zorluğu ve hatta imkânsızlığı, kolluk kuvvetleri ve yargıda dijital okuryazarlık seviyesinin düşüklüğü yer almaktadır.

c. Siber suçlarda yetkili yargı makamının belirlenmesi

Koordinasyon toplantıları sırasında özellikle savcı ve hâkimler, yetki uyuşmazlıkları nedeniyle soruşturmaların aşırı uzadığını, delillerin kaybolduğunu ve bu nedenle soruşturmaların sonuçsuz kaldığını belirtmişlerdir. Bu noktada Ceza Muhakemesi Kanununun yargı yetkisini düzenleyen 12. maddesinde bir değişiklik yapılması gerektiği düşünülmektedir. Söz konusu maddenin altıncı fıkrasında bilişim sistemleri, banka veya kredi kuruluşlarının ya da banka veya kredi kartlarının araç olarak kullanılması suretiyle işlenen suçlarda mağdurun yerleşim yerindeki mahkemelerin yetkili olduğu açıkça düzenlenmiş olmakla birlikte, bu düzenlemenin yetersiz olduğu ifade edilmiştir.

Nitekim Yüksek Yargıdan bir katılımcı da bu durumun ortaya çıktığı örneklerden biri olarak çok sayıda mağdurun bulunduğu ve her bir mağdur için düşük miktarda bir zararın söz konusu olduğu dava dosyalarını göstermiştir. Suçluların soruşturma süreçlerini engellemek için özellikle bu stratejiyi tasarladıkları açıktır.

Yetkisizlik nedeniyle dosyaların farklı bölgelerdeki savcılıklar ve mahkemeler arasında dolaşması kritik delillerin toplanmasını engellemektedir. Dolayısıyla sonuç olarak kovuşturma aşamasında tanık ifadeleri dışında toplanabilecek kayda değer bir delil kalmamaktadır.

Yetki meselesi, suçların soruşturma ve kovuşturma aşamalarındaki en önemli usullerden biri olan "delillerin toplanmasına" müdahale ettiğinden, soruşturmaların etkinliği için yetki meselesinin açıklığa kavuşturulması gerekmektedir. Bu anlamda siber suçlar için kesin yargı yerini işaret eden bir düzenleme getirilmesi önerilebilir.

d. Elektronik delillerin toplanması, paketlenmesi, muhafazası, taşınması ve incelenmesi için daha kapsamlı düzenlemelerin uygulamaya koyulması

Elektronik deliller tespit edildikleri an itibarıyla toplanmaya ve incelenmeye uygun değildir. Diğer taraftan, elektronik delillerin analizi ek zaman, emek ve uzmanlık gerektirir. Hassas, kolaylıkla tahrif edilebilir ve tamamen yok edilebilir olmaları nedeniyle bu delillerin toplanması ve incelenmesinin özel bir dikkat gerektirdiği belirtilmiştir.

Elektronik delillerin bozulabilir olması nedeniyle, bu delillere ilk temastan savcılığa veya mahkemeye sunulma anına kadar azami dikkat ve özen gösterilmelidir.

Elektronik delillerin nasıl toplanacağı, muhafaza edileceği ve aktarılacağına ilişkin bir kılavuzun bulunmaması büyük bir eksikliktir. Gerçekten de elektronik deliller siber suçların soruşturulmasında kilit bir rol oynamaktadır. Halihazırda zarar görmeye son derece açık olan bu deliller, toplama aşamasında kolluk personelinin eylemleri nedeniyle kullanılamaz hale gelmektedir. İlk elde edildiği anda yanlış kişilerce yapılan yanlış işlemlere maruz kalan bir elektronik delilin bütünlüğünün ve geçerliliğinin korunması büyük risk taşır. Bu, somut delil eksikliği nedeniyle yargılamanın ilerleyen aşamalarında soru işaretlerine neden olmakta ve bu nedenle soruşturma ve kovuşturmaların akıbetini derinden etkilemektedir.

Bu konuda kapsamlı bir yasal düzenleme bulunmadığından süreç, elektronik delilleri toplayacak kolluk personelinin inisiyatifinde yürütülmektedir. Çıkarılacak bir yasal düzenlemede elektronik delillerin toplanması sırasında uyulması gereken genel ilkeler ve zorunlu usuller, delilleri toplayacak kolluk personelinin nasıl hareket etmesi gerektiği, düzenlemeye aykırı işlemlerin ihlal olarak değerlendirileceği ve bu konuda cezai işlem yapılacağı açıkça belirtilmelidir.

Bu kapsamda elektronik delillerin toplanması sırasında yapılmasının zorunlu kılınması önerilen işlemlerden bazıları şunlardır:

• Elektronik delillerin özenli bir şekilde ve ayrı ayrı paketlenmesi,

• Elektronik delilleri belgeleme sürecinin kronolojik bir raporu olan gözetim zincirinin oluşturulması,

• Toplanan elektronik cihazların canlı analizi,

• Aktarım için kapatmadan önce elektronik cihazların şifrelerinin ve modellerinin not edilmesi,

• Elektronik cihazdaki dijital materyallerin gölge kopyasının alınması,

• Elektronik delillerin veri bütünlüğünü korumak için hash algoritmalarının (kriptografik özetleme fonksiyonu) toplanması,

• Zaman damgası.

Hâlihazırda Ceza Muhakemesi Kanununun 134. maddesi bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma şeklindeki koruma tedbirini düzenlemektedir. Elektronik delillerin toplanması süreçlerini açıklayan düzenlemenin ilgili kanun hükmü ile uyumlu bir şekilde oluşturulması elzemdir. Ayrıca elektronik delil olsun ya da olmasın, her türlü delil toplama işleminde uyulması gereken ilkeler burada da geçerli olacaktır. Nitekim olay yerinde toplanan delillerin toplanması sırasında yapılan bir hata, delilleri hukuka aykırı hale getirir ve dolayısıyla delillerin yargılamaya ve hükme esas alınmasını engeller. Özellikle çocuk pornografisi görüntüleri içeren dosyaların şüpheli veya sanığa teslim edilmesiyle ilgili olarak da aynı maddede değişiklik yapılmalıdır.

Koordinasyon toplantıları sırasında adli bilişim uzmanları ile hâkim ve savcılar arasında elektronik delillerin incelenmesine ilişkin yazışmalar konusunda da bir tartışma yapılmıştır. Elektronik delillerin incelenmesine ilişkin olarak Adli Tıp Kurumuna yazılan yazıların çok genel talepler içermesi, araştırılacak konuların spesifik olmaması, incelenmek üzere gönderilen delillerin seçilmeden gönderilmesi ve bu nedenle suçla ilgisi olmayan bilgi ve kişisel verilerin ayıklanması sırasında zaman kaybı yaşanması temel sorunlar olarak tespit edilmiştir.

e. Siber suçların soruşturma ve kovuşturma aşamalarında gönderilen taleplerin yerine getirilmesi konusunda bankaların sorumluluğu

Koordinasyon toplantılarında bankalar ile kolluk kuvvetleri, hâkim ve savcılar arasındaki iletişim trafiğinin delillerin toplanması ve suçtan doğan zararların önlenmesi üzerindeki olumsuz etkileri sıklıkla dile getirilmiştir. Özellikle bilişim teknolojileri aracılığıyla işlenen dolandırıcılık suçlarında bankalar ile adli makamlar arasındaki iş birliği büyük önem taşır. Bankalardan gelen yanıtların soruşturma ve kovuşturmaların akıbeti için ne kadar önemli olduğu, hatta soruşturmaların devamının bankalardan gelen yanıtlara bağlı olduğu açıktır. Bu doğrultuda, "hızlı yanıt" vermenin önemi vurgulanmaktadır.

Bilişim sistemleri kullanılarak işlenen dolandırıcılık suçlarının soruşturulması ve kovuşturulmasında hızlı yanıt sorunu, bankalar ile adli makamlar arasındaki

temel sorundur. İhbar ve şikâyetler adli makamlara ulaşmadan önce zaten bir zaman kaybı yaşanmaktadır. Bu zaman kaybına ek olarak, şikâyetler üzerine soruşturma açılmasından sonra bankalara yazılan soruşturma yazılarına verilen yanıtların gecikmesi, kayıtların imha edilmesi nedeniyle bankalardan delil elde edilememesine neden olmaktadır.

Bu durumun en belirgin örneklerinden biri ATM'lerin güvenlik kamerası kayıtlarının 6 ay gibi kısa bir süre için saklanması ve bu sürenin sonunda imha edilmesidir. Bu gibi durumlarda suçun işlenmesinde kullanılan banka hesaplarının bulunduğu bankaların güvenlik kamerası kayıtlarından delil elde etmek ve bu görüntüler üzerinden suçun faillerini tespit etmek imkânsız hale gelmektedir.

Aynı şekilde hesap ekstrelerine ilişkin kayıtların kısa bir süreliğine saklanması da benzer sorunlara yol açmaktadır. Hesap dökümleri incelenerek para transferlerinin tespit edilmesi mümkün olmakla birlikte, bu dökümlere ulaşmak için izlenmesi gereken prosedür çok zaman alabilmektedir. Nitekim koordinasyon toplantıları sırasında yargıdan bazı katılımcılar soruşturma ve kovuşturma aşamalarında bu tür delillerden ümitlerini kestiklerini açıkça ifade etmişlerdir.

Bankalardan delil elde edilmesindeki hız ve zaman sorunları kadar önemli bir diğer konu da banka hesaplarının bloke edilmesi sürecidir. Hesap bloke etme talepleri için adli makamlar ile bankaların iletişime geçmesi uzun zaman aldığından, mağdurların bu konuda bilinçlendirilmesi ve öncelikli olarak harekete geçmesi gerektiği ileri sürülmüştür. Ayrıca, mağdurun hesabından tutar çok hızlı bir şekilde çekildiği için hesap sahibinin şüpheli bir işlemi mümkün olduğunca çabuk bildirmesi gerektiği ifade edilmiştir.

Hesap bloke etme işlemi hızlı bir şekilde yapılmadığı takdirde dolandırıcılık yoluyla ele geçirilen para farklı hesaplara aktarılarak çekilmektedir. Buna bağlı olarak banka hesabında artık bulunmayan ve fiziki dolaşıma giren paranın geri alınması neredeyse imkânsız hale gelmektedir.

Suça konu para henüz çekilmemiş olsa bile farklı bankalar arasında transfer edilmekte ve bu transferlerin izini sürmek oldukça zorlaşmaktadır. Nitekim her bankadan alınan yanıtlarda farklı hesaplara transfer yapıldığı görülürse, transferin yapıldığı bankaya yeni bir bilgilendirme talebi yazılması gerekir. Tüm bunlar süreçleri uzatır ve mağduriyetin çözümsüz kalmasına neden olur. Bu nedenle, bankalar arası para akışları için merkezi bir çatı kuruluşun kurulması tavsiye edilebilir.

Banka hesaplarının hızlı bir şekilde bloke edilmesinin ve bankalara gönderilen yazılara aynı şekilde yanıt verilmesinin sağlanması önemlidir. Bankalara gönderilen yazılara zamanında yanıt verilmemesi ve bloke etme taleplerinin uzun bir süre sonra yapılması gibi konular açısından Birleşik Krallık örneği önemlidir. Nitekim bankalardan adli makamlara yapılan dönüşlerin gecikmesi için herhangi bir yaptırım öngörülmemesi büyük bir eksikliktir.

Dolayısıyla, bankalara tebliğ edilen sunma emirlerinin kullanılması önerilmektedir. Bu usule göre, kolluk veya adli makam, bankaya veya bir kuruma

elektronik olarak gönderilen bir emri imzalar ve onlara tam bir yanıt için süre verir. Banka veya ilgili kurumun emre uymaması halinde, bankadan bir temsilcinin yetkililerin huzuruna çıkması için talimat verilir.

Kurumların yasal taleplere yanıt verme sürelerinin iyileştirilmesine ihtiyaç olduğu açıktır ve soruşturmalarda geçen sürenin iyileştirilmesi için yaptırımlar içeren yasal bir çerçevenin uygulanması önemle tavsiye edilmektedir.

f. Fidye yazılımı kullanımının suç olarak tanımlanması

Fidye yazılımı kullanımı yeni ortaya çıkan bir siber suç olarak tanımlanmalıdır.

Fidye yazılımı saldırısı, bilgisayar sistemlerine saldırılması sonucunda ele geçirilen sisteme erişimin engellenip bu engelin kaldırılması için mağdur kullanıcılardan fidye talep edilmesini içeren bir suçtur. Fidye yazılımı saldırılarının, Türkiye'de olduğu gibi Avrupa'da da siber suçlar alanında en yaygın yöntemlerden biri olduğu ve çoğu fidye yazılımı saldırısının e-posta yoluyla gönderilen bir bağlantıya tıklanarak gerçekleştirildiği bilinmektedir. Bu yeni suç türünün genellikle tespit edilemediği veya sınıflandırılamadığı açıktır.

Bu suçun mağdurları, özellikle de şirketler istenen fidyeyi öderken, diğerleri bilgisayar sistemlerini güncellemeyi tercih etmektedir. Bu çok yeni bir olgu olmasına rağmen, bu tür saldırılar günümüzde olağan kabul edilmektedir. Zayıf politikalar, sistem kurulumları ve koruma önlemlerinin eksikliği nedeniyle şirketler zor kararlar vermek durumunda kalırken, bireyler de çeşitli belgelerini geri almak için fidye ödemeye razı olmaktadır. Dolayısıyla, fidye yazılımı mağdurları genellikle bu suç nedeniyle kolluk kuvvetlerine veya adli makamlara ihbar veya şikâyette bulunmamaktadır. Bunu bir virüs saldırısı olarak algılama ve kendi başlarına çözüm arama eğilimindedirler. Ayrıca koordinasyon toplantıları sırasında adli bilişim uzmanları tarafından fidye yazılımlarının çok çeşitli olduğu belirtilmiştir. Bu suça müdahale özel uzmanlık gerektirmektedir.

Fidye yazılımlarının ceza kanunları kapsamında yeni bir suç olarak tanımlanması ve uygun yaptırımların sağlanması büyük önem taşır. Bu suç kendine özgü eylemleri ile mevcut diğer siber suçlardan ayrılmakta ve daha ağır cezalar gerektirmektedir. Bu suçun ihdas edilmesinin ardından soruşturma ve kovuşturma aşamalarında uluslararası bir iş birliği ağının kullanılması gerekliliği vurgulanmalıdır. Fidye yazılımlarının uluslararası alanda işlenebilen bir suç olması, bu suçla mücadelede uluslararası iş birliğini önemli kılmaktadır. Zira bu suç, dünyanın herhangi bir yerinden İnternet üzerinden gönderilen bir e-posta veya mesaj yoluyla işlenebilmekte ve failin yabancı bir ülkede, mağdurun ise başka bir ülkede olduğu senaryolarda suçun soruşturulması ve kovuşturulması çok daha zorlu bir hal almaktadır.

g. Siber Uşaklaştırmanın bir suç olarak tanımlanması

Çocukların çevrim içi ortamlarda taciz edilmesi (siber kölelik / çevrim içi istismar) yeni ortaya çıkan bir siber suç olarak tanımlanmalıdır.

Geleneksel istismar suçlarının işlenmesinde bilişim sistemlerinin kullanılması ve faillerin bu sistemler aracılığıyla mağdurlara kolaylıkla ulaşabilmesi nedeniyle siber uşaklaştırma daha yaygın hale gelmiştir. Özellikle çocukları hedef alan bu suç yaygınlaşmaktadır. Tanım olarak siber uşaklaştırma , bir yetişkinin çoğunlukla cinsel sömürü veya istismar amacıyla bir çocuk veya ergenle çevrim içi ilişki kurmasıdır. Ancak bunu sadece cinsel istismarla sınırlandırmak doğru olmaz. Mağdur çeşitli şekillerde taciz edilebilir. Örneğin "Mavi Balina" adlı bilgisayar oyununda mağdurlar kendilerine zarar vermeye hatta intihara teşvik edilmiştir.

Çeşitli ülkelerde siber uşaklaştırma ayrı bir suç olarak sınıflandırılmasa da cinsel bütünlüğe karşı işlenen suçlar kapsamında düzenlenmektedir. Örneğin Birleşik Krallık'ta çocuklara karşı taciz suçu, çevrim içi platformlar aracılığıyla işlenenler de dâhil olmak üzere çeşitli cinsel suçların ele alındığı 2003 Cinsel Suçlar Yasası kapsamında yer almaktadır. Benzer şekilde, Fransa'da siber uşaklaştırma, Fransız Ceza Kanununun cinsel suçlara ilişkin hükümleri, özellikle de çocukların korunması ve cinsel şiddetle mücadeleye ilişkin hükümleri kapsamında ele alınmaktadır.

Bu bağlamda, siber uşaklaştırma ile ilgili çeşitli eylemleri cezalandırmayı öngören cezai hükümler olsa bile, bu yeni suçun diğer siber suçlardan ayrılması ve siber uşaklaştırma suçunun istismarla ilgili mevcut suçların ağırlaştırılmış ve nitelikli bir şekli olarak ceza kanunlarına dâhil edilmesi önemle tavsiye edilmektedir. Aslında Lanzarote Sözleşmesinde de siber uşaklaştırmanın ele alınması ve bununla mücadele edilmesi gerektiği vurgulanmaktadır.

h. Yeni düzenlemelerin getirilmesi gerekliliği

Veri Koruma yönetmeliği ve siber güvenlikle ilgili mevcut mevzuat, siber suçlarla mücadele için yeterli yasal dayanak sağlamamaktadır. Kolluk kuvvetlerinin veri işleme faaliyetleri için yasal dayanak eksiktir ve siber güvenlikle ilgili mevcut hukuki çerçeve dağınıktır ve uygulamada da zorunlu ve etkili olmaktan uzaktır. Bunlara paralel olarak, siber olaylara ilişkin kritik deliller tamamen karanlıkta kalma tehlikesiyle karşı karşıya kalmakta, kolluk kuvvetlerinin veri toplama uygulamaları yasal dayanak ve yeterli güvencelerin olmaması nedeniyle hukuka aykırı kabul edilmektedir.

Bu nedenle, kamu sektöründe ve özel sektörde siber olayların bildirilmesini zorunlu kılacak yasal düzenlemelerin ve kapsayıcı bir siber güvenlik mevzuatının hazırlanması önerilmektedir. Ayrıca, kamu ve kolluk faaliyetlerinde kişisel verilerin işlenmesine ilişkin mevzuatı düzenleyerek temel haklara saygılı bir şekilde siber suçlarla mücadeleye yasal dayanak sağlayan eksiksiz bir düzenlemeye ihtiyaç duyulmaktadır.

3. Kolluk Kuvvetleri

Üçüncü paragrafta yer alan yorumlar ve tartışmalar, çalıştaylardaki katılımcıların tartışmalarına dayanmaktadır. Uluslararası Uzmanlar tarafından, Avrupa'daki diğer ülkelerde ve başka yerlerde çalışma deneyimlerine dayanarak herhangi bir tavsiyenin uygulanmasının potansiyel değerini gösteren bazı yorumlar eklenmiştir. Bu yorumların yapıldığı yerler dipnotlarda belirtilmiştir.

a. Ulusal Siber Suç Biriminin (USSB) oluşturulması

Hâlihazırda Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı, siber suçları soruşturmakta ve/veya teknolojinin bir suç veya ilgili deliller için önemli bir faktör olduğu konularda Polis ve Savcılıktaki diğer kurumlara destek vermek için adli uzmanlık sağlamaktadır.[2]

Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı aynı zamanda uluslararası ve ulusal hizmet sağlayıcılarla veri bildirme taleplerine ilişkin 7/24 Tek İrtibat Noktasını (7/24 TİN) da bünyesinde barındırmaktadır.

Koordinasyon toplantıları sırasında, siber suçlarla mücadeleye liderlik edecek ulusal bir birimin oluşturulması gerektiği konusunda fikir birliğine varılmıştır. Bu liderlik, cezai kovuşturmaları desteklemeye yönelik soruşturmalar ve adli bilişim faaliyetleri ile sınırlı kalmamalı, aşağıdaki gibi diğer önemli alanlarda da liderliği içerecek şekilde genişletilmelidir:

- En ciddi ve önemli siber suçların soruşturulması,
- Siber suç altyapılarının bozulması ve dağıtılması,
- Türkiye'yi etkileyen yeraltı ekonomisi çalışmalarının önlenmesi ve bunlarla mücadele edilmesi,
- Ülkedeki Jandarma, bölgesel ve yerel polis siber suç birimleriyle iş birliği içinde çalışmalar yürütülmesi,
- USOM (Ulusal Siber Olaylara Müdahale Merkezi), üniversiteler vb. gibi paydaşlarla ortak çalışmalar yürütülmesi,
- Siber suçların önlenmesi,
- Siber suçları, çevrim içi zorbalığı ve benzer sorunları azaltmaya yönelik farkındalık kampanyaları,
- Bilgi güvenliği sektörüyle ilişkiler,
- Teknik uzmanlık,
- İstihbarat yönetimi ve paydaşlarla siber suçlar hakkında istihbarat paylaşımı,
- Uluslararası ilişkiler,
- Uzman soruşturma becerileri (Karanlık Ağ'daki suç forumlarına yönelik gizli soruşturma ve kripto para soruşturmaları gibi),
- 7/24 TİN,

[2] https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/turkey/pop_up#:~:text=The%20National%20Cybercrime%20Department%20of,a%20crime%20or%20related%20evidence.

• Siber suç soruşturmalarında ve elektronik delillerin ele alınmasında iyi uygulamaların teşvik edilmesi.

Siber suçlar ve elektronik delillerle ilgili ulusal meselelere odaklanan bağımsız bir yapıya sahip olması, önemli cezai soruşturmalar yürütmesi ve teknoloji destekli suçların etkisini azaltmak için çalışan pek çok ortakla iş birliği yapması gereken bir USSB'nin kurulması Türkiye'yi Avrupa'daki diğer pek çok ülkede bulunan sistemle daha da uyumlu hale getirecektir [3].

Birçok USSB'de kullanılan beceriler sadece Polis yetkilerine sahip olanlarla sınırlı olmayıp, diğer teknik ve endüstriyel uzmanlarının istihdamı yoluyla katma değer elde edilmektedir.

b. Çocuklara yönelik çevrim içi istismar alanında görev yapan bir birimin oluşturulması

Çevrim içi cinsel istismara maruz kalan çocukların ilk ihbarlarıyla ilgili sorunlar, koordinasyon toplantılarına katılan çeşitli taraflarca gündeme getirilmiştir. Bir toplantıda Uluslararası Çocuk Merkezinden (Ankara) bir temsilci, mevcut ihbar sisteminin çocuklara yönelik fiziksel veya çevrim içi cinsel istismarın ihbar edilmesini desteklemediğini, çünkü hassas veya gizli ihbar yöntemlerinin bulunmadığını belirtmiştir.

Toplantılarda yapılan görüşmelerde, diğer Avrupa ülkelerinde çocuklara yönelik fiziksel ve cinsel istismarın bildirilmesi için özel internet sitelerinin kullanıldığı ve yetkililerin, genç mağdurları destekleyen çocuk yardım kuruluşları ve destek kuruluşlarından ihbar almaya hazır oldukları tespit edilmiştir.

Bu soruşturmalarda, çocukların yaşadıkları travmatik olaylar hakkında tekrar tekrar ifade verme ihtiyacını azaltan video şeklindeki ifadelerin kullanılması da tartışılmıştır.

Yapılan tartışmalarda, Türkiye'nin Çocukların Cinsel Suistimal ve Cinsel İstismara Karşı Korunmasına İlişkin Avrupa Konseyi Lanzarote[4] Sözleşmesini (Türkiye'de 1 Nisan 2012'de yürürlüğe girmiştir[5]) imzalarken yaptığı anlaşmaların birçoğunun, çevrim içi ortamda meydana gelen bu tür suçların soruşturulması veya mahkemelerdeki duruşmaları sırasında ya yürürlükte olmadığı ya da uygulanmadığı tespit edilmiştir.

Çocukların korunmasının, Türkiye'deki Sosyal Medya hizmet sağlayıcıları ile etkileşim yoluyla geliştirilebileceği tespit edilmiştir. Diğer yorumlarda, çevrim içi ortamda gençlere yönelik çocuk istismarı ve zorbalık konularının ele alınmasına ilişkin kapsamlı bir stratejinin eksikliğinden bahsedilmiştir.

[3] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.
[4] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1de
[5] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=201

Her ne kadar Emniyet Genel Müdürlüğü ve Jandarma, okullarda zorbalığı, cinsel içerikli şantajı ve çocukların kendi çektikleri cinsel görüntülerin dolaşımını önlemeye yönelik olan yerel önleme kampanyalarıyla başarılı vaka çalışmaları sunmuş olsa da; bazı delegeler, çocuklara yönelik çevrim içi cinsel istismar ve zorbalık ile ilgili olarak ülke genelinde daha yapılandırılmış bir farkındalık kampanyasının düzenlenmesini önermiştir.

Ulusal Çocuk İstismarı ve Çevrim İçi Koruma Biriminin (veya benzer bir birimin) oluşturulması mevcut durumu iyileştirebilir. Böyle bir birim oluşturulmalı ve bildirilen eksikliklerin birçoğunu gidermekle görevlendirilmelidir. Böyle bir birim, yukarıdaki yorumlara ek olarak aşağıdakileri sağlamalıdır[6]:

• Çocukların çevrim içi cinsel istismar ve zorbalığı bildirmeleri için uzman bir çevrim içi sistem.

• Mağdurları desteklemek ve kurtarmak ve failleri tespit etmek ve kovuşturmak için çevrim içi çocuk istismarı soruşturmasında uzmanlaşmış savcılar,

• Çocukların çevrim içi cinsel istismarının soruşturulması, mağdurların belirlenmesi ve kurtarılması ve karanlık ağdaki gizli platformlarda faaliyet gösteren şüphelilerin belirlenmesine yönelik gizli soruşturma becerileri,

• Hükümete Türkiye'de çocuklara yönelik çevrim içi cinsel istismar tehdidi hakkında güncel ve ilgili verilerin sağlanması ve neden olunan zararın azaltılmasına yönelik stratejik önerilerin sunulması.

Türkiye'de kurulacak Ulusal Çocuk Sömürüsü ve Çevrim İçi Koruma Birimi (veya benzer bir birim) bağımsız bir yapıya sahip olmalı ve Çocukların Çevrim İçi Ortamlarda Cinsel İstismarı ve Sömürüsü ile ilgili ulusal konulara odaklanmalıdır. Bu birim önemli cezai soruşturmaları yürütebilirken, polis yetkileri dışında, eğitimli danışmanlara ve travma geçirmiş çocuklarla görüşme yapmak üzere eğitilmiş kişiler gibi başka donanımlı personele de sahip olmalıdır.

c. Siber suçlar için çevrim içi bir ulusal ihbar merkezinin oluşturulması

Sekiz koordinasyon çalıştayının tamamında yapılan görüşmelerde, kolluk kuvvetleri ve savcılar tarafından ele alınan siber suç ve teknoloji destekli suç ihbarlarında önemli bir artış olduğu tespit edilmiştir. İhbar edilen siber suçların 2020'den itibaren her yıl %10-20 oranında arttığına dair göstergeler sunulmuştur. Siber suç birimlerinden sorumlu birçok kıdemli memur, artan personel ve kaynakların iş yükü seviyelerini karşılamadığını belirtmiştir. Suç ihbarı ve soruşturması için daha etkili yöntemlerin gerekli olduğunu ifade etmişlerdir.

Savcılar, siber suç vakalarının genellikle doğrudan savcılığa ihbar edildiğini, bu nedenle iddiaları anlamak için özel bir görüşme yapılmasını gerektiğini belirtmişlerdir. Savcıların iş yükü nedeniyle bu tür görüşmeler genellikle randevu

[6] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.

ile gerçekleşmekte ve toplantı sonrasında savcılar ilgili elektronik delillerin koruma altına alınması için kolluk kuvvetlerini yönlendirebilmektedir. Elektronik delillerin koruma altına alınması ve ele geçirilmesindeki bu tür gecikmelerin soruşturmaları aksattığı bilinmektedir.

Olayların Polise bildirildiği durumlarda, Polis verileri koruma altına alma imkânına sahipti ve bunu olay bildirilir bildirilmez yapabilmekteydi. Bu kapasite mevcut olmakla birlikte, bu tutarsız bir şekilde uygulanmaktaydı. (bkz. paragraf 3d).

Bir çalıştayda, bir hâkim tarafından sunulan bir vaka çalışması, fail tarafından benzersiz bir telefon numarası kullanılması nedeniyle hâkimin diğer davaları nasıl birbirine bağladığını göstermiştir. Hâkim, kendisine sunulan dizinleri nasıl araştırdığını açıklamış ve toplantının katılımcıları için faydalı bilgiler sağlamıştır. Ancak siber suçlar için ulusal bir ihbar merkezinin oluşturulması, Türkiye'de ihbar edilen tüm olaylarda failler hakkındaki bilgileri kaydetmek için özel bir sistemin uygulamaya koyulmasını sağlayacaktır. Bu bilgilerin analizi ve elektronik delillerin hızlı bir şekilde koruma altına alınması işlemleri zamanında yapılabilir ve daha sonra bilgi ve deliller bir siber soruşturma birimine ve uygun bir savcıya iletilebilir.

Siber suçlar için ulusal ihbar merkezlerinin nasıl oluşturulacağına dair çeşitli örnekler ve bu merkezlerin oluşturulmasının faydaları INTERPOL ve Avrupa Konseyinin "Siber Suçlar ve Elektronik Delillere İlişkin Ceza Adaleti İstatistikleri Rehberi"[7][8] adlı yayınlarında ayrıntılı olarak açıklanmıştır.

d. Eğitim ve uzmanlık becerileri

Tüm koordinasyon çalıştayları sırasında polis ve yargıda önemli beceri eksiklikleri olduğu tespit edilmiştir. Polis teşkilatında elektronik delillerin aranması ve ele geçirilmesi konusunda ön saflarda görev yapan polisler için eğitime ihtiyaç duyulduğu ve siber suç birimlerinde elektronik deliller, yazılımlar, kötü amaçlı yazılımlar, kripto paralar ve karanlık ağ gibi daha karmaşık konuların soruşturulmasını desteklemek için uzmanlık becerilerine ihtiyaç duyulduğu tespit edilmiştir.

Siber suçların soruşturulması ve elektronik delillerin ele alınması konusunda eğitim eksikliklerinin ilgili tüm kamu kurumlarında mevcut olduğu sıklıkla tartışılmıştır. Ayrıca, siber suçlarla mücadeleye ilişkin kaynakların (ulusal ve yerel) nasıl arttığı, ancak ihbar edilen suçların seviyesine kıyasla yeterli olmadığı anlatılmıştır. Bütçeler ve yeni personelin eğitimi çeşitli zorluklara neden olmuştur. Tüm etkinliklerde kripto para ve karanlık ağ soruşturmaları konusunda eğitime ihtiyaç duyulduğu belirtilmiştir.

[7] https://www.interpol.int › content › download › file
[8] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.

Tespit edilen diğer zorluklar arasında personelin görev değiştirmesi ve siber suç alanının dışına çıkması yer almaktadır. Bu, eğitime yapılan yatırımın boşa gittiği ve yeni memurların onların yerini alması gerektiği manasına gelmektedir ki bu da ilgili becerileri korumak için daha fazla eğitim ve tecrübeye dayanan öğrenmenin gerekli olduğu anlamını çıkarmaktadır.

Eğitim ihtiyacı ile ilgili birçok önemli konu tartışılmış olsa da, sürdürülebilir kapasite geliştirme için anlamlı bir eğitim planı veya yol haritası ortaya koyulmamıştır. Kolluk kuvvetlerinin bütüncül bir eğitim stratejisi uygulaması ve buna personeli elde tutma planlarını da dâhil etmesi **tavsiye edilmektedir.** Avrupa Konseyi (Interpol ile ortaklaşa), Siber Suçlar ve Elektronik Deliller Hakkında Kolluk Kuvvetleri Eğitim Stratejilerinin Geliştirilmesi Kılavuzunu yayımlamıştır.[9] Bu belgede şöyle denmektedir: "*İyi hazırlanmış bir stratejik plan, siber suçlar ve elektronik deliller gibi çok katmanlı ve karmaşık sorunlara yanıt vermede çok önemli bir rol oynayabilir. Ancak, sadece stratejik bir belgenin varlığı yeterli değildir.*

Stratejiler ancak biri kurumun üyeleri ve paydaşları arasında sürekli iletişim yoluyla kurum kültürünün bir parçası haline geldiklerinde yararlı olurlar. Stratejilerin etkili olabilmesi için aynı zamanda kurumun ihtiyaçlarına dayalı olarak belirlenmesi ve bu ihtiyaçlara cevap vermesi gerekir; bu ihtiyaçlar da ilgili paydaşlarla geniş tabanlı istişareler yapılarak belirlenmelidir."

Türkiye'de uygulamaya koyulacak herhangi bir eğitim stratejisi, devriye memurlarından deneyimli memurlara ve siber suç uzmanlarına kadar tüm görevlerdeki memurların ihtiyaçlarına yönelik olmalıdır.

Avrupa Konseyi tarafından Hukukçular için İnsan Hakları Eğitimine ('HELP') yönelik çevrim içi eğitim platformu aracılığıyla sağlanan bazı eğitim materyalleri hâlihazırda mevcuttur. HELP'ye kayıt olmak için https://help.elearning.ext.coe.int/login/index.php adresinden basit bir kayıt işlemi yapmanız gerekmektedir. Şu anda, Türkiye'de ceza adaleti sisteminin güçlendirilmesine yönelik Avrupa Birliği - Avrupa Konseyi Ortak Projesi kapsamında Türkçeye çevrilmiş olan ve tamamlanması on saat sürecek olan siber suç soruşturmasına ilişkin dokuz eğitim modülü bulunmaktadır.[10]

Diğer eğitim gereksinimleri arasında, devriye gezerken veya karakolda görev yaparken siber suç ihbarı alan polis memurları için rehberlik sağlanması da yer alıyordu, zira elektronik delillerin korunması veya ele geçirilmesi için yapılması gereken basit işlemler yapılmamaktadır ve bu da suçluların başarılı bir şekilde kovuşturulması fırsatlarının kaybedilmesine neden olmaktadır. Bu sorunla ilgili olarak Avrupa Konseyi "siber suç soruşturmalarına ilk müdahale edenlere yönelik rehber" adlı bir kılavuz hazırlamış ve yayımlamıştır.[11]

[9] https://rm.coe.int/guide-for-developing-training-strategies-final/1680a62c72
[10] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.
[11] https://www.coe.int/en/web/octopus/training#{%2264860563%22:[5]}

Türkiye'ye daha fazla destek vermek amacıyla iPROCEEDS-2 projesi kapsamında Ocak 2022'de 100'den fazla katılımcıya kılavuzun açıklandığı iki günlük bir çevrim içi sunum yapılmıştır. Türkiye'nin bu kılavuzu bir şablon olarak kullanarak ön saflarda görev yapan polis memurlarına ve soruşturmacılara bu eğitimi vermeye devam etmesi **tavsiye edilmektedir**[12].

e. Ağır iş yükü

Çalıştaylarda, hacmi ve karmaşıklığı sürekli artan siber suçlar ve elektronik delillerle ilgili ağır iş yükü sürekli olarak dile getirilmiştir. Bu talepleri karşılamak için kaynakların yetersiz olduğu şeklinde yorumlar yapılmıştır. Polis ve Savcılar genellikle daha fazla personel, kaynak, kabiliyet ve eğitime ihtiyaç duyduklarını belirtmişlerdir.

Diğer paralel tartışma konuları arasında siber suç soruşturmalarının yürütülmesi için gereken zaman ve değişmeyen iç sürtüşmeler yer almıştır. Savcıların inanılmaz bir iş yükü vardır ve davaları çözmek için Kolluk Kuvvetlerine ve diğer üçüncü taraflara çok sayıda talep ve müzekkere gönderirler. Kolluk Kuvvetlerinin de kaynaklara yönelik yüksek talepleri vardır ve suç iddialarına ve Savcılardan gelen taleplere mümkün olduğunca çabuk yanıt vermeye çalışırlar. Bu soruşturmaları yürütmek için bankalar, İSS'ler, telekomünikasyon şirketleri vb. gibi üçüncü taraflara bilgi talepleri gönderirler. Bu üçüncü tarafların kolluk kuvvetlerinden (ve savcılardan) gelen taleplere yanıt verecek özel birimleri bulunmamakta, bu da daha fazla gecikmeye neden olmaktadır. Sonuç olarak, teorik olarak aylar içinde tamamlanabilecek davaların sonuçlanması genellikle yıllar almaktadır.

Türkiye çok gelişmiş bir ülke ve G20 üyesi olmasına rağmen, ek kaynakların devreye sokulmasının Devlete ve dolayısıyla vergi mükelleflerine bir maliyeti vardır. Türkiye, diğer birçok ülke gibi kaynaklarını etkin bir şekilde yönetmek ve kamu sektöründe yapılan mali yatırımlardan önemli sonuçlar almak zorundadır. Mevcut durumu iyileştirmek için iş yükünün verimli ve etkin bir şekilde yönetilmesi ve bazı zor ve çetrefilli kararların alınması gerekmektedir.

Avrupa Konseyi uzmanları, çalıştaylar sırasında uluslararası bir perspektiften, birçok siber suç vakasının klasik tepkisel soruşturma teknikleri kullanılarak çözülemeyeceği konusunda genel bir bakış açısı sunmuştur. Küçük kayıplara yol açan siber suçların çözülmesi için orantısız kaynak ayrılması gibi başka faktörler de söz konusudur. Çözülme olasılığı düşük olan ya da soruşturulmaya değmeyecek kadar az mali kayıp yaratan suçların elenerek soruşturulmaması için Savcılık ve Polis arasında bir iş birliği anlaşması yoluyla bir eleme sisteminin uygulamaya koyulması **tavsiye edilmektedir**[14].

[12] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.
[13] https://www.g20.org/en/about-g20/
[14] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.

Ayrıca, herhangi bir eleme kararı verildiğinde, bir siber suç ister elenmiş isterse tamamen soruşturulmuş olsun, her bir vakanın olgularının istihbarat ve istatistiksel raporlama için kullanılması **önemle tavsiye edilmektedir.**

f. Kurumlar arası iş birliği

Tüm çalıştaylar boyunca yapılan önemli tartışmalar ve yorumlar, kurumlar arası iş birliğinin gözden geçirilmesi ve geliştirilmesi gerektiğini göstermiştir. Bu durum, İhtiyaç Değerlendirme Raporunda siber suçların soruşturulmasında görev alan farklı kurumlar arasındaki koordinasyon konusunda sunulan tavsiyede göz önünde bulundurulmuştur.

Çalıştaylara katılanlar, Emniyet Genel Müdürlüğü ve Jandarma arasında bilgi ve istihbarat paylaşımının zayıf olduğu yorumunda bulunmuşlardır. Katılımcılardan gelen diğer yorumlarda da kolluk kuvvetleri ve savcılar arasındaki iletişimde benzer eksiklikler gündeme getirilmiştir. Bu iletişim ve iş birliği kasıtlı gibi görünmemekle birlikte, siber suçlar ve elektronik deliller konusunda paydaşlar arasında bölgesel ve ulusal düzeyde çok az iletişim olduğu belirtilmiştir. Örneğin, ilk çalıştaylarda tespit edilen pek çok sorun diğer yedi çalıştayda da tekrarlanmıştır. Merkezi bir noktada, bu sorunları toplayacak, çözümleri belirleyecek ve çareleri uygulamaya koyacak bir mekanizma olmadığı görülmüştür.

Çalıştaylara katılan ve tartışmalardan yararlanarak gündeme getirilen konularla ilgilenilmesi için uygun faaliyetleri uygulamaya koyan Adalet Bakanlığına müteşekkiriz. Örnekler arasında bankaların güvenlik kamerası görüntülerini daha uzun süre saklamasına ilişkin değişiklikler, kullanıcısı tespit edilemeyen cep telefonları (patates hatlar) konusuna ilişkin düzenlemelerin iyileştirilmesine yönelik adımlar ve adli bir görüntü elde edildikten sonra dijital delillerin eski haline getirilmesine ilişkin mevzuatın değiştirilmesine yönelik planlar (Ceza Muhakemesi Kanunu Madde 134) yer almaktadır.

Türkiye'de kurumlar arası iş birliğine ilişkin olarak geçmişte gerçekleştirilen diğer faaliyetler, EGM siber suç birimleri, mali soruşturma birimleri, MASAK ve savcılık gibi paydaşlarla çevrim içi suç gelirlerinin aranması, el koyulması ve müsaderesine ilişkin toplantıların düzenlendiği 3 ve 4 Nisan 2017 tarihine kadar uzanmaktadır. Çeşitli tavsiye ve anlaşmaları içeren Türkiye Kurumlar Arası İş Birliği Protokolü başlıklı belge o zaman hazırlanmıştır ve bugün de geçerliliğini korumaktadır. Etkinlikle ilgili ayrıntılar Avrupa Konseyi Siber Suçlar sitesinde[15] bulunabilir. Belgenin tamamı talep üzerine Bükreş'teki iPROCEEDS-2 projesinden temin edilebilir[16].

Bazı kilit sonuçlar ve anlaşmalar aşağıdaki gibidir:

• Cezai soruşturmalar sırasında iş birliği

[15] https://www.coe.int/en/web/cybercrime/-/iproceeds-workshops-on-inter-agency-and-international-cooperation-for-search-seizure-and-confiscation-of-online-crime-procee-1
[16] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.

• Ulusal önlemler

• Uluslararası önlemler

• İstihbarat, bilgi ve delil paylaşımı

• Çok kurumlu gruplar

• Kamu-özel sektör iş birliği

• Uluslararası iş birliği

• İstatistikler

• Kurumlar arası iş birliğine yönelik protokollerin hazırlanmasına ilişkin tavsiyeler.

g. Siber suçlar için proaktif becerilerin geliştirilmesi

Gizli izleme ve genellikle özel tedbirler olarak tanımlanan diğer soruşturma tekniklerinin kullanımı, organize suçların soruşturulmasında kolluk kuvvetlerinin becerilerinin kilit bir alanıdır. Telefon dinleme, gizli soruşturmacı, test alımları ve çevrim içi ortamda gözetlemeyi içeren bu tedbirlerin kullanımı, siber suçlara karşı ulusal müdahaleyi tamamlamak için gereklidir.

Bu teknikler, suç forumları ve sohbet odaları gibi diğer çevrim içi kaynaklardan şüpheliler ve failler hakkında bilgi ve delil toplamak için kullanılabilir. Gizli bir soruşturmada (İnternette veya gerçek dünyada) görev alan herkes her zaman uygun şekilde eğitilmiş, yetkin ve yetkili olmalıdır. Böyle bir soruşturmanın gizli ve izlenemez bir şekilde yürütülmesi için gerekli ekipman ve ilgili hizmetlerin tedarik edilmesi göz önünde bulundurulmalıdır. Ekipman veya hizmetlerin hiçbirinin hiçbir koşul altında bir kolluk kuvvetine kadar izlenmesi mümkün olmamalıdır.

Gizli faaliyetlerin merkezi olarak özel bir birimde konumlandırılmasını ve gerektiğinde soruşturmalara destek vermek üzere gerçekleştirilmesini tavsiye ederiz. Gizli bir görevde çalışırken birçok zorluk vardır; örneğin memurlar uygun etik standartlara bağlı kalmalıdır. Bilgi toplarken, soruşturmaya konu olan kişiyle temas kurarken ve bu teması sürdürürken ilk görevlendirme talimatlarında belirtilen koşullara uygun hareket etmelidirler.

Gizli Soruşturmacı:

• Eylemlerinin yasal sınırlarını belirleyebilmelidir (neyin suça iştirak oluşturduğunu anlayabilmek de dâhil);

• Delilleri doğrulama ihtiyacını iyice anlamalıdır;

• Soruşturulan kişinin ve soruşturmadan etkilenen diğer tüm tarafların İnsan Hakları üzerindeki etkilerini dikkate almalıdır.

Bu yetkililerin merkezi bir birime yerleştirilmesiyle, faaliyetleri amir ve müdürler tarafından yakından izlenebilir. Gerekli kontrol ve gözetimi sağlamak için özel standart çalışma usulleri geliştirilebilir.

Gizli soruşturmacılar, soruşturmayla ilgili tüm materyallerin her zaman dayanıklı ve geri alınabilir bir biçimde saklanmasını ve kaydedilmesini sağlamalıdır. Bu, normalde EGM veya Jandarma bünyesinde bulunmayan güvenli sistemlerin geliştirilmesini gerektirebilir[17].

h. Suç önleme ve farkındalık

Çalıştaylar sırasında katılımcılar suçun önlenmesi ve farkındalık kampanyalarının önemini kabul etmişlerdir. Bu kadar çok siber suç karşısında, sadece siber suçluların kovuşturulmasının suç düzeylerini azaltmayacağı kabul edilmiştir. Aktarılan bazı örnekler şunlardır:

• Çocukların siber suç (ve çevrim içi istismar) mağduru olmalarını önlemeye yönelik faaliyetler başlatılmalıdır;

• İnsanların para katırı ya da yasa dışı mal teslim noktası olarak hareket ederek suça sürüklenmelerine ilişkin genel bilgilendirme kampanyaları;

• Mağdurların siber suçları nasıl ihbar edeceklerini bilmeleri için farkındalık yaratılması.

Emniyet Genel Müdürlüğü ve Jandarma, zorbalık, cinsel taciz ve çocukların pornografik görüntülerinin yayılmasını önlemek için farklı bölgelerdeki okullarda yürüttükleri önleme kampanyalarına ilişkin örnek çalışmalar sunabilmiştir. Bunlar bir miktar etki yaratmış olsa da, siber suçları azaltmaya yönelik tutarlı bir stratejik planın eksikliği ortadadır.

Türkiye Ulusal Siber Güvenlik Stratejisinde şöyle denmektedir: "*Toplumun tüm kesimlerinde siber güvenlik kültürünün yerleşmesi çağın gereklerinden biridir. Bu kültürün temeli ise yüksek düzeyde farkındalığın sağlanmasına dayanmaktadır. Teknolojinin güvenli kullanımının önemi tüm bireyler tarafından benimsendiğinde, riskler ve tehditlerin hayata olumsuz etkileri gözle görülür biçimde azalacaktır.*

Bu bağlamda bireysel, kurumsal ve ulusal ölçeklerde, yani tüm toplum genelinde, farkındalığı artırıcı çalışmaların gerçekleştirilmesi; aileler, çocuklar, öğrenciler, gençler, kadınlar, yaşlılar ve engellilere yönelik faaliyetlerle her kesime ulaşılması öncelikli hedefler arasında yer almaktadır. Çocukların siber ortamda korunmasına yönelik farkındalık kampanyaları ve ailelere düşen sorumluluklara ilişkin bilinç düzeyini artırıcı etkinlikler de bu kapsamda önem derecesi yüksek çalışmalar olacaktır[18]."

Stratejinin başka bir yerinde ise şöyle denmektedir: "*Siber suçlarla mücadele yöntemlerinin sürekli geliştirilmesi, önleyici, caydırıcı ve etkili çalışmalar yapılması gerekmektedir. Bu bağlamda 2020-2023 döneminde de siber suçla mücadelenin*

[17] Bu son iki paragraf, uluslararası uzman(lar) tarafından yapılan yorumlardır.
[18] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf - sayfa 24

daha güçlü şekilde sürdürülmesi için bu alandaki ulusal kapasitenin ve teknolojik imkânların artırılması amaçlanmaktadır[19]*."*

Bu stratejik hedeflere ulaşmak için **kolluk kuvvetlerinin** ulusal ve yerel düzeyde mesajların nasıl verileceğini içeren **bütüncül bir siber suç önleme planı oluşturması önerilmektedir**. Bu plan kaynakların en etkin şekilde kullanılmasını sağlamalı, mükerrerliği önlemeli ve yürütülen faaliyetlerin ölçülmesini sağlamalıdır.

İdeal olarak hem ulusal hem de yerel düzeylerde **siber suçların önlenmesine odaklanacak özel birimlerin oluşturulması tavsiye edilmektedir**.

Diğer birçok ülkede siber suçlar ve mağdur olmaktan kaçınmanın yolları hakkında halka bilgi sağlayan çevrim içi kaynaklar bulunmaktadır. Bunlar, ulusal siber olaylara müdahale merkezleri (USOM gibi) tarafından oluşturulan kamu bilgilendirme mesajlarına ek olarak sunulmaktadır. Çalıştaylarda tartışılan bir örnek, Birleşik Krallık'taki, Get Safe Online (https://www.getsafeonline.org) adlı İnternet sitesidir. **Türk Hükümetinin kolluk kuvvetleriyle iş birliği içinde benzer bir kaynak oluşturması** ve bunu günlük değişikliklere göre güncel tutması **önemle tavsiye edilmektedir.** Diğer pek çok ülke, Get Safe Online'dan kişilerle doğrudan etkileşimin iyi bir başlangıç noktası sağladığını tespit etmiştir ve benzer ulusal oluşumların oluşturulması konusunda tavsiyelerde bulunmaktadır[20].

i. 7/24 Tek İrtibat Noktası

Her çalıştayda sosyal medya şirketlerinin rolü ve talep edilen bilgi ve delillerin Polise düzenli olarak sağlanamaması gündeme gelmiştir. Polis ve Savcılar dolandırıcılık ve hakaret davalarıyla ilgili konularda talepte bulunduklarında bilgi ve delil talepleri genellikle cevapsız kalmaktadır. Genel olarak, sosyal medya şirketlerinin tam ve zamanında bilgi sağladığı tek alanın çocuk istismarı ve çocuklara yönelik cinsel istismar materyallerine ilişkin davalar olduğu tespit edilmiştir.

Hakaret ve diğer benzer suç türlerinin Türkiye dışındaki pek çok ülkede genellikle 'ifade özgürlüğü' ile medeni hukuk (ceza hukukundan ziyade) arasında sıkışıp kaldığı delegelere sürekli olarak açıklanmıştır. Dolayısıyla bu ülkelerde, hakaret davaları ve diğer davalarla ilgilenilmesini sağlayacak, karşılıklı adli yardım ve mütekabiliyetin temel taşı olan cezai bir çerçeve bulunmamaktadır. Dolayısıyla herhangi bir soruşturmanın başarısız olması kaçınılmazdır. Bu durumun yaygın bir şekilde yanlış anlaşıldığı görülmektedir ve savcılar ve yargı arasında, başarısızlığa mahkûm talepleri önlemek amacıyla durumu netleştirmek için anlamlı bir eyleme ihtiyaç vardır.

[19] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf - sayfa 26

[20] Bu paragraf, uluslararası uzman(lar) tarafından yapılan bir yorumdur.

DDiğer yorumlar, Türkiye dışındaki Sosyal Medya şirketlerinden bilgi almanın zorlukları, suç teşkil eden hesapların kapatılmaması veya ele geçirilen hesaplarla yeteri kadar ilgilenilmemesi ile ilgilidir. Birçok delege, erişimin sadece Türkiye sınırlarına kadar uzandığını kabul etse de mevzuatın gerekli olduğunu düşünmektedir.

Elektronik delillerle ilgili tartışmalarda, bu delillerin günlük süreçlerin veya suç faaliyetlerinin bir parçası olarak hızla değiştirilebildiği, silinebildiği, taşınabildiği veya üzerine yazılabildiği tespit edilmiştir. Çevrim içi verilerin (e-postalar, sunucular, iletişim verileri vb.) koruma altına alınması faaliyeti yaygın olarak anlaşılmamaktadır ve acil koruma talepleri yeterince etkin bir şekilde yerine getirilmiyor gibi görünmektedir. Verilerin korunmasına ihtiyaç duyulduğu durumlarda, 7/24 Tek İrtibat Noktası (7/24 TİN) yeterince kullanılmamıştır. Çeşitli çalıştaylarda yapılan tartışmalara göre bunun iki ana nedeni vardır:

• Yetkilinin, 7/24 TİN'nin sağlayabileceği hizmetler hakkında bilgi sahibi olmaması;

• Yetkilinin 7/24 TİN'ye nasıl ulaşacağını bilmemesi.

Eğitim ve 7/24 TİN'nin iletişim bilgilerinin daha geniş bir şekilde paylaşılmasını bu durumu iyileştirebilir.

Sosyal Medya şirketlerinin Türkiye'de nasıl hareket ettiğini ve 7/24 TİN'nin rolünü açıklamak için elektronik delillerle ilgilenen 7/24 Tek İrtibat Noktasının rolü hakkında çevrim içi bir eğitim ve talimatların verilmesi tavsiye edilmektedir. Bu etkinliklerin ve iletişim çalışmalarının amacı, çok uluslu hizmet sağlayıcıların ve sosyal medya şirketlerinin Türkiye'ye hangi materyalleri ve talepleri göndermeye hazır olduklarını belirlemek ve başarısız olmaya mahkûm talep türlerini tespit etmektir.

7/24 TİN'nin iletişim bilgileri asgari olarak tüm savcılar ve siber suç birimleriyle (hem EGM hem de Jandarma) paylaşılmalıdır.

4. Savcılar

a. Siber suçlarla mücadelede savcıların rolü

Türkiye'de savcıların siber suçlarla mücadeledeki rolü çok yönlü ve çok önemlidir. Devletin yasal temsilcisi olarak savcı, siber suç işlediğinden şüphelenilen kişileri soruşturmak, suçlamak ve kovuşturmaktan sorumludur.

Bu süreçte birçok farklı aşama vardır ve savcılar için iyi uygulama protokolü aşağıda yer almaktadır:

1. Soruşturma: Savcılar delil toplamak, şüphelileri tespit etmek ve siber suçlu olduğu iddia edilen kişilere karşı güçlü bir dava oluşturmak için kolluk kuvvetleri ve siber suç birimleriyle iş birliği yaparlar. İlgili bilgileri elde etmek için İnternet servis sağlayıcıları ve teknoloji şirketleri gibi özel sektör ortaklarıyla da çalışabilirler.

2. İddianameler: Savcılar soruşturma sırasında toplanan delillere dayanarak, şüphelilere karşı resmî suçlamalarda bulunup bulunmayacaklarına karar verirler. Suçun niteliği, neden olunan zararın ciddiyeti ve şüphelinin suç geçmişi gibi faktörleri göz önünde bulundurarak uygun iddianameleri hazırlamaktan sorumludurlar.

3. 3.Kovuşturma: Savcılar, mahkeme işlemlerinde devleti temsil ederler ve sanığın suçluluğunu kanıtlamak için delil ve savları sunmaktan sorumludurlar. Mağdurlar ve toplum için adaleti sağlarken sürecin sanık için adil ve hakkaniyetli olmasını ve sanığın haklarının ihlal edilmemesini sağlamalıdırlar.

4. İş birliği: Siber suçlarla mücadele genellikle uluslararası iş birliğini gerektirir, çünkü siber suçlular sınırlar ötesinde faaliyet gösterebilirler. Savcılar, bilgi paylaşmak, soruşturmaları koordine etmek ve gerektiğinde ortak kovuşturma yürütmek için diğer yargı bölgelerindeki meslektaşlarıyla birlikte çalışmalıdır.

5. Hukuki uzmanlık: Savcılar, siber suçlarla ilgili yürürlükteki yasalar ve hukuki çerçeveler hakkında derin bir anlayışa ve aynı zamanda yeni eğilimler ve teknolojiler konusunda güncel bilgilere sahip olmalıdır. Bu bilgiler, yasaları etkili bir şekilde uygulamalarına ve sürekli gelişen siber suç ortamına uyum sağlamalarına yardımcı olur.

6. Önleme ve caydırıcılık: Savcılar, siber suçları kovuşturarak ve mahkûmiyet kararı verilmesini sağlayarak, muhtemel suçluların benzer faaliyetlerde bulunmaktan caydırılmasına katkıda bulunurlar. Ayrıca, siber suçlarla ilgili hukuki sonuçlar konusunda halk arasında farkındalık yaratarak potansiyel suçluların bu tür davranışlarda bulunmasını önleyebilirler.

7. Savunuculuk ve politika geliştirme: Savcılar, siber suçlarla mücadele için daha güçlü yasaların, politikaların ve kaynakların savunulmasında rol oynarlar. Siber suç davalarını ele alırken edindikleri deneyim ve içgörülere dayanarak yasa koyuculara ve politika yapıcılara değerli fikirler sağlayabilirler.

8. Kapasite geliştirme: Savcılar, siber suçlarla mücadelede kolluk kuvvetlerinin, yargının ve diğer paydaşların etkinliğini artırmayı amaçlayan kapasite geliştirme çalışmalarına katılırlar. Bu, eğitim ve öğretim programlarını, en iyi uygulamaların paylaşılmasını ve ilgili ve uygun kılavuz ve protokollerin geliştirilmesini içerebilir.

b. Savcıların siber suç kovuşturmalarında karşılaştıkları zorluklar

Savcıların karşılaştığı zorlukları tespit etmek amacıyla Türkiye'nin çeşitli coğrafi bölgelerinde koordinasyon toplantıları gerçekleştirilmiştir. Savcıların siber suçların soruşturulması ve kovuşturulmasıyla nasıl ilgilendikleri konusunda bazı ortak sorunlar ve bazı bölgesel farklılıklar tespit edilmiştir. Bu toplantılara katılım yüksek olmuş ve başlıca zorluklar aşağıdaki şekilde belirlenmiştir:

Teknik karmaşıklık

Savcılar arasında siber suç davalarıyla ilgilenirken beceri ve bilgi eksikliği olduğu yaygın olarak kabul edilmiş ve onaylanmıştır. Siber suçlar genellikle

sürekli gelişen karmaşık teknolojiler ve yöntemler içerir ve bu, eğitim almadıkları sürece savcıların altta yatan mekanizmaları anlamalarını ve delilleri açık ve öz bir şekilde sunmalarını zorlaştırır. Ayrıca, davanın teknik yönlerini hâkim ve/veya mahkeme heyetine açıklamak için uzmanlara bağımlılık söz konusudur.

Bu nedenle, savcıların elektronik delillerin ve diğer dijital delillerin ele alınması da dâhil olmak üzere tüm siber suçlar konusunda düzenli güncellemelerle eğitim almaları gerekmektedir. Böylece siber suçlar ve elektronik deliller konusundaki bilgilerini geliştirmeye devam edebilirler.

Çalıştaylarda güvenilir bilirkişi sıkıntısı yaşandığına dikkat çekilmiş, bu iddiaya adli bilişim uzmanı bilirkişi tarafından itiraz edilmiştir. Bilirkişi, savcıların genellikle belirsiz ve muğlak delil talepleri sunduklarını, delilleri uygunsuz bir şekilde paketlediklerini ve şifreler gibi ek bilgi taleplerine derhal yanıt vermediklerini belirtmiştir. Savcıların genellikle kafa karıştırıcı buldukları adli bilişim raporlarını daha iyi anlayabilmeleri için eğitim almaları önerilmiştir. Adli bilişim uzmanları da belki bir terimler sözlüğü ve görseller ekleyerek ifadelerini basitleştirmeye çalışmalıdır. Adli bilişim uzmanları, deneyimlerini ve en iyi uygulamaları paylaşmaları için çevrim içi bir ağ kurulmasını önermiştir.

Savcıların adli bilişim uzmanlarına delil göndermeleri için bir şablon oluşturulması tavsiye edilmiştir. Adalet Bakanlığı böyle bir şablon geliştirme sürecindedir.

Savcılar ayrıca savcılık dosyaları için kullanılan değerlendirme sisteminden de bahsetmişlerdir. Bu sisteme göre savcılar ele aldıkları davaların miktarına göre değerlendirilmektedir. Bu sistem, siber suç davalarından ziyade saldırı veya hırsızlık gibi küçük davalarla ilgilenmeyi teşvik etmektedir. Bunun nedeni, uzmanlık becerileri gerektiren, genellikle uluslararası unsurlar içeren ve çözülmesi önemli ölçüde daha uzun süren siber suç davalarının karmaşıklığıdır. Siber suç davalarına bakan savcıların terfi ettirilmesine yönelik mevcut değerlendirme sistemi genellikle yönettikleri ve başarıyla sonuçlandırdıkları dava sayısına bağlıdır. Siber suç davalarını soruşturmak için gereken uzun süre göz önüne alındığında, bu davalara bakan savcılar, davaları yeterince hızlı sonuçlandıramadıkları için orantısız bir şekilde etkilenmektedir.

Bu durum savcıların kariyer ilerlemelerini etkilediğinden, siber suç davalarının bu temel performans göstergesinin kapsamından çıkarılması ya da siber suç davalarının karmaşıklığı nedeniyle diğer davalardan daha yüksek puanlanması veya derecelendirilmesi tavsiye edilmiştir. Adalet Bakanlığı bunun hem savcıları hem de hâkimleri etkileyen bir sorun olduğunu kabul etmiştir ve bu sorunu çözmek için olası çözümleri araştırmaktadır.

Sorunun bir kısmı da savcıların ilgilenmesi gereken çok fazla dava olmasıdır.

Diğer ülkelerde ne olduğuna bakmak faydalı olacaktır. Örneğin Birleşik Krallık'ta sistem farklıdır çünkü hâkimler ve savcılar dava dosyası üzerinde çalışmazlar. Bunun yerine bu iş kolluk kuvvetleri tarafından yapılır. Birleşik

Krallık'ta savcı soruşturma aşamasında davayla ilgili danışmanlık ve rehberlik sağlar. Hangi yetkilerin devredilebileceğini görmek için savcıların çalışmalarının incelenmesi önerilmiştir. Örneğin, ilgili eğitimleri almış memurlar tanık ve mağdur ifadelerini alabilirler. Birleşik Krallık'ta özellikle de elektronik delillerin ele geçirilmesi ve duruşmalarda kullanılması konusunda ceza adaleti personelinin eğitimi ve becerilerinin artırılması gerçekleşmiştir. Örneğin, polis tarafından video görüşmesi yapılması, mağdur ve/veya tanığın kimliğinin uygun olduğunda gizlenmesi gibi uygulamalar dâhil olmak üzere, hassas materyallerle (çocukların cinsel istismarına ilişkin materyaller) ve savcılığın (ve soruşturmanın) çocuk istismarı mağdurlarıyla ilgilenme biçimiyle ilgili eğitimler verilmiştir.

Adalet Bakanlığı, savcıların asli işlerini yapabilmeleri için savcının hangi görevlerinin başkalarına devredilebileceğini değerlendirmiştir. Savcılara, uygun görevleri devredebilecekleri yardımcılar atanacaktır.

Tek irtibat noktasının olması

Savcılar, özel işletmelerin, bankaların ve hizmet sağlayıcıların bilgi taleplerine yanıt vermediklerini tespit etmiştir. Bu da davalar üzerinde olumsuz bir zincirleme etki yaratmaktadır. Sonuç olarak, işletmeler, polis ve savcıların aktif irtibat ve yardımı kolaylaştırmak için tek bir irtibat noktasının olması önerilmiştir.

Dijital delillerin toplanması ve koruma altına alınması

Dijital delillerin 'uçucu' olması ve kolaylıkla değiştirilebilmesi veya yok edilebilmesi nedeniyle bu delillerin toplanması ve korunması zor olabilir. Savcılar, dijital delillerin uygun şekilde toplanmasını, korunmasını ve analiz edilmesini sağlamak için kolluk kuvvetleriyle yakın iş birliği içinde çalışmalıdır.

İhbar edilen siber suçların sayısında önemli bir artış olmuştur ve elektronik delillerin yetkin bir şekilde ele alınması için adli bilişime olan ihtiyaç artmıştır. Savcılar ve Adli Tıp Kurumu arasında nelerin gerekli olduğu konusunda genel bir iletişim ve rehberlik eksikliği olduğu görülmüştür. Bu koşullar altında, taraflar arasında daha iyi iletişim ve rehberlik gereklidir. Delillerin toplanmasına ilişkin şablon ve kılavuzlarla sistemdeki eksikliklerin giderilmesine yardımcı olunması tavsiye edilmiştir.

Suç faaliyetlerinde kullanılan IBAN numaralarına ilişkin olarak UYAP ile entegre bir veri tabanı oluşturulması önerilmiştir. IBAN ve hesap bilgilerinin UYAP sistemi üzerinden kolluk kuvvetleri ve/veya savcılıkların kullanımına sunulması önerilmiştir.

Yargı bölgeleri arası sorunlar

Siber suçlular genellikle uluslararası sınırların ötesinde faaliyet göstermekte, bu da yargı yetkisi ve yasaların uygulanmasıyla ilgili yasal zorluklar yaratabilmektedir. Suçluların iadesi, karşılıklı adli yardım ve farklı ülkeler arasında iş birliği konusunda kolluk kuvvetleri yavaş ve karmaşık görevler yürütebilir.

Anonimlik ve şifreleme

Siber suçlular kimliklerini ve konumlarını gizlemek için genellikle anonim ağlar ve şifreleme gibi araçlar ve teknikler kullanırlar. Bu durum şüphelilerin izinin sürülmesini, kimliklerinin tespit edilmesini ve önemli delillere ulaşmayı zorlaştırabilir.

Şifreleme ile ilgili olarak, şifrelenmiş veya başka bir şekilde erişilemeyen bilgilerin şifresini vermeyi reddeden bir kişinin bu eylemini suç sayan Birleşik Krallık'ın 2000 tarihli Soruşturma Yetkileri Yasası (RIPA) Bölüm 49 Düzenlemeleri ile ilgili bir tartışma yapılmıştır. Bu mevzuata duyulan ilgi ifade edilmiş ve toplantı sırasında bir delege bu mevzuatın İnsan Hakları mevzuatına aykırı olmadığına dair şaşkınlığını dile getirmiştir. Bölüm 49 Birleşik Krallık'ta 2007 yılından beri yürürlüktedir ve İrlanda Cumhuriyeti, Fransa, Avustralya ve Finlandiya gibi ülkelerde de benzer bir mevzuat bulunmaktadır. Bu tür yetkilerin hepsinde koruma önlemleri vardır ve bunlar gereklidir. Bu husus bir tavsiye niteliğinde olmayıp, uluslararası ortakların şifreleme gibi zorluklarla nasıl başa çıktıklarını inceleyen tartışmaları yansıtmaktadır.

Hızla gelişen teknoloji

Teknolojinin hızlı gelişimi, kanunların ve kanun uygulama tekniklerinin yeni siber suç türlerine ayak uydurmakta zorlanabileceği anlamına gelmektedir. Savcıların ortaya çıkan eğilimlerden haberdar olmaları ve stratejilerini buna göre uyarlamaları gerekmektedir. Bunu da uygun bir eğitimle yapabilirler.

Hukuki çerçeveler

Siber suç yasaları yargı bölgeleri arasında farklılık gösterir ve bazı durumlarda mevcut yasalar güncelliğini yitirmiş veya yeni siber suç türlerini ele almak için yetersiz olabilir. Savcılar yasaları etkili bir şekilde uygulamada zorluklarla karşılaşabilir ve hukuki çerçevede başarılı kovuşturmayı engelleyen boşluklar olabilir.

CMK'nin 134. maddesinin (bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma) yetersizliği konusunda herkes hemfikirdir.

Kaynak kısıtlılıkları

Siber suçların kovuşturulması yoğun kaynak gerektirebilir ve bu kaynaklara özel beceriler, bilgiler ve araçlar dâhildir. Kolluk kuvvetleri ve savcılıklar, siber suçları etkili bir şekilde soruşturmak ve kovuşturmak için gerekli kaynak, eğitim ve personelden yoksun olabilir. Örneğin, kripto para davalarındaki paraları takip ederken, teknolojinin oldukça hızla değiştiği ve ayak uydurmanın zor olduğu yaygın olarak kabul edilmektedir. Bu durum, aşağıdaki 4c bölümünde belirtildiği üzere uzmanlık eğitiminin önemini daha da öne çıkarmaktadır.

Kamu farkındalığı ve mağdur bildirimi

Birçok siber suç mağduru hedef alındığının farkında olmayabilir ya da utanç,

korku veya yetkililere olan güvensizlik nedeniyle suçu ihbar etme konusunda isteksiz olabilir. Bu durum savcıların güçlü davalar oluşturmasını ve siber suçluları adalete teslim etmesini zorlaştırabilir. Bu konuyla ilgili daha fazla tartışma için aşağıdaki 8b bölümüne bakabilirsiniz.

Niyetin belirlenmesi ve isnat

Suç niyetini kanıtlamak ve siber suçları belirli kişilere isnat etmek, çevrim içi faaliyetlerin genellikle anonim olması nedeniyle zor olabilir. Savcılar, sanığın bilerek suç teşkil eden faaliyetlerde bulunduğunu ve eylemlerinden sorumlu tutulabileceğini göstermek için yeterli delili toplamalıdır.

c. Savcılar için uzmanlık eğitimi ve kaynakların önemi

Çalıştaylar, siber suç davalarıyla ilgilenen savcıların geleneksel hukuk eğitimlerinin ötesinde uzmanlık eğitimine ihtiyaç duyduklarını ortaya koymuştur. Eğitim ihtiyaçları düzenli olarak gözden geçirilmeli ve siber suçlarla ilgili hizmet içi eğitim çalışmaları sürekli olarak yürütülmelidir. Siber suçlarla ilgili eğitimler, standart hizmet öncesi eğitim müfredatının ayrılmaz bir parçası olmalıdır. Savcılar (ve hâkimler ve kolluk kuvvetleri) için kapsamlı bir eğitim stratejisi olmalıdır. Her savcı, siber suçlarla ilgili delil teşkil eden tüm konularla etkin bir şekilde ilgilenebilmelidir.

Savcıların siber suçlarla ilgili bilgilerini uygulayabilmeleri için bu tür eğitim programlarında kurgusal duruşmalar gibi pratik uygulama fırsatları sunulmalıdır.

Bu amaçla, iProceeds-II projesi kapsamında hazırlanan Elektronik Delillere İlişkin Olarak Adli Personele Yönelik Uzmanlık Eğitimi Türkçeye çevrilmiş ve Türkiye'nin hukuki çerçevesine uyarlanmıştır. Bunun yakın gelecekte hem savcılar hem de hâkimler için Adalet Akademisinin eğitim programlarına entegre edilmesi hedeflenmektedir.

Savcıların ek eğitime ihtiyaç duyabilecekleri tespit edilen alanlardan bazıları şunlardır:

1. Siber suç yasalarının anlaşılması: Savcıların ulusal ve uluslararası siber suç yasalarını tam olarak anlamaları çok önemlidir. Bu, ilgili ulusal mevzuatın yanı sıra Avrupa Konseyinin Budapeşte Siber Suç Sözleşmesi gibi daha geniş kapsamlı uluslararası sözleşmelere aşina olunmasını içerir.

2. Teknik bilgi: Savcıların siber suçların teknolojik yönlerini kavraması gerekir. Bu, adli bilişim, ağlar, bilgisayar donanımları, kötü amaçlı yazılımlar, fidye yazılımları, kimlik avı, kripto para birimi ve karanlık ağ ve diğer siber suç araçları ve yöntemlerinin nasıl kullanıldığının anlaşılmasını içerir.

3. Dijital delillerin kullanılması: Eğitim, dijital delillerin toplanmasını, korunmasını ve analizini kapsamalıdır. Bu, dijital deliller için gözetim zincirinin nasıl sürdürüleceğinin, adli bilişim uzmanlarıyla nasıl çalışılacağının ve bu tür delillerin mahkemede nasıl sunulacağının anlaşılmasını içerir. Bu aynı zamanda hassas materyallerin ele alınmasını ve savunmanın erişimine açılmasını da içerir.

4. Siber suç eğilimlerinin ve taktiklerinin anlaşılması: Sürekli eğitimler, teknolojinin hızlı gelişimi göz önüne alındığında en son siber suç eğilimleri, taktikleri ve tehditlerinin yanı sıra bunlarla mücadele etmek için kullanılan araç ve stratejilere ilişkin güncellemeleri de içermelidir.

5. Uluslararası ve yargı bölgeleri arası sorunlar: Siber suçlar genellikle birden fazla yargı bölgesini kapsadığından, savcıların uluslararası mevzuat ve suçluların iadesi anlaşmaları ve diğer ülkelerdeki kolluk kuvvetleriyle etkili bir şekilde nasıl iş birliği yapılacağı konusunda eğitime ihtiyaçları vardır.

6. Mağdur desteği: Siber suçların mağdurlar üzerinde önemli duygusal ve mali etkileri olabilir. Savcıların mağdurlara nasıl etkili destek ve kaynak sağlayabilecekleri konusunda eğitim almaları gerekmektedir.

5. Hâkimler

a. Siber suçlarla mücadelede hâkimlerin rolü

Türkiye'de hâkimlerin siber suçlarla mücadeledeki rolü çok yönlü ve önemlidir. Adalet sisteminin yasal bir temsilcisi olarak bir hâkim, uzun bir kovuşturma sürecinde siber suç işlediğinden şüphelenilen kişiler hakkında karar vermekten sorumludur.

Bu süreç farklı aşamalardan oluşmaktadır ve hâkimler için iyi uygulama protokolü aşağıda yer almaktadır:

1. Soruşturma: Hâkimler, kovuşturma aşamasının yanı sıra soruşturma aşamasının da bir parçasıdır. Soruşturma aşamasında savcılar, siber suçlularla ilgili delillerin toplanması konusunda hâkim kararıyla koruma tedbiri talep etme yetkisine sahiptir.

2. İddianame ve takipsizlik kararı: Savcılar soruşturma sırasında toplanan delillere dayanarak, şüphelilere karşı resmî suçlamalarda bulunup bulunmayacaklarına karar verirler. Bu kararla birlikte iddianameler hâkimler tarafından yasal gereklilikler açısından incelenir. Hâkimler, daha detaylı bir soruşturma süreci sağlayarak ya da savcıların iddianamelerindeki eksikliklerin giderilmesini talep ederek iddianamenin iadesine karar verebilirler. Öte yandan savcılar, siber suç işlediği iddia edilen kişilerin suç işlediğine dair yeterli delil olmadığı düşüncesiyle takipsizlik kararı verebilmektedir. Takipsizlik kararları da davanın taraflarından herhangi birinin itirazı doğrultusunda hâkimler tarafından incelenmektedir.

3. Kovuşturma: Hâkimler, mahkeme işlemlerinde devleti temsil ederler ve tarafların tüm iddialarını ve savunmalarını incelemekten ve kamu kurumlarıyla ve özel kuruluşlarla iş birliği içinde eksik ve talep edilen delilleri toplamaktan sorumludur. Ana görevleri ise tüm bu süreçlerin sonunda, tüm tarafların haklarının adil ve hukuka uygun bir şekilde korunduğu ve saygı duyulan bir karar vermektir.

4. İş birliği: Siber suçlarla mücadele genellikle uluslararası iş birliğini gerektirir,

çünkü siber suçlular sınırların ötesinde faaliyet gösterebilirler. Hâkimler, bilgi paylaşmak, kovuşturmaları koordine etmek ve gerektiğinde ortak kovuşturma yürütmek için diğer yargı bölgelerindeki meslektaşlarıyla birlikte çalışmalıdır.

5. Hukuki uzmanlık: Hâkimler, siber suçlarla ilgili yürürlükteki yasalar ve hukuki çerçeveler hakkında derin bir bilgiye ve aynı zamanda yeni eğilimler ve teknolojiler konusunda güncel bilgilere sahip olmalıdır. Bu bilgiler, yasaları etkili bir şekilde uygulamalarına ve sürekli gelişen siber suç ortamına uyum sağlamalarına yardımcı olur.

6. Önleme ve caydırıcılık: Hâkimler, siber suçları kovuşturarak ve siber suçlular hakkında adil karar vererek siber suçlarda cezasızlığın önlenmesine katkıda bulunurlar. Ayrıca, hakkaniyet temelinde verdikleri kararlarla siber suçlarla ilgili hukuki sonuçlar konusunda halk arasında farkındalık yaratırlar.

7. Savunuculuk ve politika geliştirme: Hâkimler, siber suçlarla mücadele için daha güçlü yasaların, politikaların ve kaynakların savunulmasında rol oynarlar. Siber suç davalarını ele alırken edindikleri deneyim ve içgörülere dayanarak yasa koyuculara ve karar vericilere değerli fikirler sağlayabilirler. Ayrıca, yüksek yargı hâkimleri özellikle emsal kararların oluşturulmasında rol oynarlar ve genel olarak hukuk sisteminin tüm tarafları için değerli hukuki görüşler sağlayabilirler. Emsal kararlar, yasal boşlukların doldurulması için de kullanılabilir ve bu açıdan gereklidir.

8. Kapasite geliştirme: Genellikle kararlarıyla konuşan hâkimler, siber suçlarla mücadelede kolluk kuvvetlerinin, yargının ve diğer paydaşların etkinliğini artırmayı amaçlayan kapasite geliştirme çalışmalarına da katılırlar. Bu, eğitim ve öğretim programlarını, en iyi uygulamaların paylaşılmasını ve ilgili ve uygun kılavuz ve protokollerin geliştirilmesini içerebilir.

b. Hâkimlerin siber suç davalarını karara bağlarken karşılaştıkları zorluklar

Hâkimlerin karşılaştığı zorlukları ortaya koymak amacıyla Türkiye'nin çeşitli coğrafi bölgelerinde koordinasyon toplantıları düzenlenmiştir. Hâkimlerin siber suçların soruşturulması ve kovuşturulmasıyla nasıl ilgilendikleri konusunda bazı ortak sorunlar ve bazı bölgesel farklılıklar tespit edilmiştir. Bu toplantılara katılım yüksek olmuş ve başlıca zorluklar aşağıdaki şekilde belirlenmiştir:

Teknik karmaşıklık

Hâkimler arasında siber suç davalarıyla ilgilenirken beceri ve bilgi eksikliği olduğu yaygın olarak kabul edilmiş ve onaylanmıştır. Siber suçlar genellikle sürekli gelişen karmaşık teknolojiler ve yöntemler içerir ve bu, eğitim almadıkları sürece hâkimlerin altta yatan mekanizmaları anlamalarını ve delilleri açık ve öz bir şekilde sunmalarını zorlaştırır. Bu eksikliğe ek olarak, çalıştaylarda güvenilir bilirkişi eksikliği dile getirilmiştir. Sonuç olarak, hâkimler için uzmanlaşmaya ihtiyaç vardır. Yakın zamanda siber suçlar için ihtisas mahkemelerinin kurulması; adli işlemlerin hızlandırılması gibi çeşitli faydalar sağlamaktadır.

Bu nedenle, hâkim ve savcıların elektronik delillerin ve diğer dijital delillerin ele alınması da dâhil olmak üzere tüm siber suçlar konusunda düzenli güncellemelerle eğitim almaları gerekmektedir. Böylece siber suçlar ve elektronik deliller konusundaki bilgilerini geliştirmeye devam edebilirler. Bu ihtiyaç, yetersiz soruşturma süreçlerinden kaynaklanmaktadır. Neredeyse tüm toplantılarda, yetersiz soruşturma süreçleri nedeniyle kovuşturma aşamasında delil toplama faaliyetleri gibi soruşturma usullerinin hâkimler tarafından yerine getirilmesi gerektiği belirtilmiştir. Hâkimlerin kovuşturma aşamasında soruşturma işlemlerini yerine getirmek için ilgili usul yetkileri olsa bile, dijital delillerin uçucu olması ve genellikle kısa bir süreliğine saklanması nedeniyle siber suç davaları için bu oldukça faydasız bir uygulamadır.

Hâkimler ayrıca siber suç davalarının nihai kararla kapatılmasına ilişkin puanlama yöntemini, karşılaşılan zorluklar ve siber suçlarda uzmanlık bağlamında tartışmışlardır. Bu zorluklar sürecin uzamasına neden olmakta ve bu davalarla ilgilenen hâkimler yeterli sayıda davayı sonuçlandıramadıkları için mağdur olmaktadır. Bu nedenle, performans değerlendirmelerinde siber suç davalarının diğer dava türlerinden farklı bir şekilde değerlendirilmesi önerilmiştir.

Tek irtibat noktasının olması

Kovuşturma aşamasında soruşturma işlemlerinin yürütülmesi gerekliliği ve yetersiz soruşturma durumu gibi yukarıda açıklanan faktörler nedeniyle kamu kurumları ve özel kuruluşlarla iş birliği ihtiyacı kovuşturma aşamasında da devam etmektedir. Dolayısıyla kovuşturmalar özel işletmeler, bankalar ve hizmet sağlayıcıların yanıt vermemesinden veya yetersiz yanıt vermesinden etkilenmektedir. Bu durum, özel aktörlere müteakip bilgi taleplerinin gönderilmesine ve kovuşturma aşamasının daha da uzamasına neden olmaktadır. Sonuç olarak, bu taraflar arasında aktif irtibat ve yardımı kolaylaştırmak için tek bir irtibat noktasının olması önerilmiştir.

Dijital delillerin toplanması ve koruma altına alınması

Yukarıda açıklandığı üzere, dijital deliller çoğu zaman soruşturma aşamasında tam olarak toplanamadığından, hâkimler ilgili yetkileri ile kovuşturma aşamasında dijital delilleri toplamakla yükümlüdürler. Ancak dijital deliller çoğunlukla suçun işlendiği tarihten aylar veya yıllar sonraki aşamalara kadar tamamen silinmekte ve ortadan kaldırılmaktadır.

Yargı bölgeleri arası sorunlar

Siber suçlular genellikle uluslararası sınırların ötesinde faaliyet göstermekte, bu da yargı yetkisi ve yasaların uygulanmasıyla ilgili yasal zorluklar yaratabilmektedir. Suçluların iadesi, karşılıklı adli yardım ve farklı ülkeler arasında iş birliği konusunda kolluk kuvvetleri yavaş ve karmaşık olabilir.

Buna ek olarak, bazı uluslararası özel kuruluşların farklı nedenlere bağlı olarak istinabe taleplerine cevap vermedikleri görülmektedir. Örneğin, hakaret

fiili Türkiye'de suç olarak düzenlenmişken, bazı Avrupa ülkelerinde bu fiil suç olarak düzenlenmemiştir. Ülkeler arasında standart bir düzenleme olmaması, uluslararası iş birliği sürecinin aksamasına neden olmaktadır.

Hızla gelişen teknoloji

Teknolojinin hızlı gelişimi, kanunların ve kanun uygulama tekniklerinin yeni siber suç türlerine ayak uydurmakta zorlanabileceği anlamına gelmektedir. Hâkimlerin ortaya çıkan eğilimlerden haberdar olmaları ve stratejilerini buna göre uyarlamaları gerekmektedir. Bunu da uygun bir eğitimle yapabilirler. Ayrıca, bu konuda yüksek mahkemelerin yakın tarihli içtihatlarını takip etmenin çok önemli olduğu bildirilmiştir. Buna paralel olarak, Ulusal Yargı Ağı Bilişim Sistemi (UYAP) ekranından izlenebilecek güncel ve ilgili içtihatları içeren haftalık veya aylık bültenler hazırlanmasının faydalı olacağı belirtilmiştir.

Hukuki çerçeveler

Siber suç yasaları yargı bölgeleri arasında farklılık gösterir ve bazı durumlarda mevcut yasalar güncelliğini yitirmiş veya yeni siber suç türlerini ele almak için yetersiz olabilir. Hâkimler yasaları etkili bir şekilde uygulamada zorluklarla karşılaşabilir ve hukuki çerçevede başarılı kovuşturmayı engelleyen boşluklar olabilir. CMK'nin 134. maddesinin (bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma) yetersizliği konusunda herkes hemfikirdir.

Ayrıca, adli makamların çeşitli koruma tedbirlerine karar verme yetkisinden yoksun olduğu belirtilmiştir. Özellikle işlemlerin dondurulması konusunda hızlı ve yeterli bir iletişim kanalının kurulması ve farkındalık artırıcı faaliyetlerin yürütülmesi gerektiği ifade edilmiştir. Buna ek olarak, adli makamların koruma tedbirleri konusunda karar vermekte oldukça çekingen davrandıkları yönünde görüş belirtilmiştir. Hesap ve işlemlerin dondurulması konusunda daha hızlı ve yeterli koruma önlemleri içeren bir yöntemin benimsenmesi gerektiği de ifade edilmiştir.

Kaynak kısıtlılıkları

Siber suçların kovuşturulması yoğun kaynak gerektirebilir ve bu kaynaklara özel beceriler, bilgiler ve araçlar dâhildir. Hâkimler, siber suçları etkili bir şekilde kovuşturmak için gerekli kaynak, eğitim ve mahkeme personelinden yoksundur. Örneğin, kripto para davalarında para takibi yapılırken teknolojinin oldukça hızla değiştiği ve ayak uydurmanın zor olduğu yaygın olarak kabul edilmektedir. Bu nedenle, bazı katılımcılar mahkemelerde ve kolluk kuvvetlerinde teknik personel görevlendirilmesini önermiştir.

Niyetin belirlenmesi ve isnat

Suç niyetini kanıtlamak ve siber suçları belirli kişilere isnat etmek, çevrim içi faaliyetlerin genellikle anonim olması nedeniyle zor olabilir. Eksik delillerin olduğu yetersiz bir soruşturmada hâkim, itham edilenin bilerek suç teşkil eden

faaliyetlerde bulunduğunu ve eylemlerinden sorumlu tutulabileceğini göstermek için yeterli delili toplamalıdır.

Tüm İhtisas Mahkemelerinin Birleştirilmesi

Toplantılarda, Türkiye'nin her ilindeki ilk derece mahkemelerinde siber suçlar konusunda ihtisas mahkemeleri kurulmasının hâkimlerin uzmanlaşmasına kesinlikle yardımcı olacağı sıklıkla dile getirilmiştir. Ancak, özellikle Ağır Ceza Mahkemeleri hâkimlerinin cinayet veya uyuşturucuyla ilgili suçlar gibi başka kritik davaları da vardır ve bu suçlar çoğu zaman hâkimlerin omuzlarına o kadar yük bindirmektedir ki siber suç davaları için gerekli çabayı gösterememektedirler. Bu nedenle, Asliye Ceza Mahkemeleri ve Ağır Ceza Mahkemelerinin yetki alanına giren tüm bilişim suçlarının tek bir ihtisas mahkemesi tarafından görülmesi ya da büyük şehirlerde siber suçlar konusunda ihtisaslaşmış Ağır Ceza Mahkemelerinin sadece siber suçları davalarına bakmasının sağlanması, böylece diğer suçların yarattığı yükün ortadan kaldırılması ve gerçek bir ihtisaslaşmanın sağlanması önerilmiştir.

c. Hâkimler için uzmanlık eğitimi ve kaynakların önemi

Çalıştaylar, siber suç davalarıyla ilgilenen hâkimlerin geleneksel hukuk eğitimlerinin ötesinde uzmanlık eğitimine ihtiyaç duyduklarını ortaya koymuştur. Eğitim ihtiyaçları düzenli olarak gözden geçirilmeli ve siber suçlarla ilgili hizmet içi eğitim çalışmaları sürekli olarak yürütülmelidir. Siber suçlarla ilgili eğitimler, standart hizmet öncesi eğitim müfredatının ayrılmaz bir parçası olmalıdır. Hâkimler (ve savcılar ve kolluk kuvvetleri) için kapsamlı bir eğitim stratejisi olmalıdır. Her hâkim, siber suçlarla ilgili delil teşkil eden tüm konularla etkin bir şekilde ilgilenebilmelidir.

Hâkimlerin siber suçlarla ilgili bilgilerini uygulayabilmeleri için bu tür eğitim programlarında kurgusal duruşmalar gibi pratik uygulama fırsatları sunulmalıdır.

Bu amaçla, iProceeds-II projesi kapsamında hazırlanan Elektronik Delillere İlişkin Olarak Adli Personele Yönelik Uzmanlık Eğitimi Türkçeye çevrilmiş ve Türkiye'nin hukuki çerçevesine uyarlanmıştır. Bunun yakın gelecekte hem savcılar hem de hâkimler için Adalet Akademisinin eğitim programlarına entegre edilmesi hedeflenmektedir.

Hâkimlerin ek eğitime ihtiyaç duyabilecekleri tespit edilen alanlardan bazıları şunlardır:

1. Siber suç yasalarının anlaşılması: Hâkimlerin ulusal ve uluslararası siber suç yasalarını tam olarak anlamaları çok önemlidir. Bu, ilgili ulusal mevzuatın yanı sıra Avrupa Konseyinin Budapeşte Siber Suç Sözleşmesi gibi daha geniş kapsamlı uluslararası sözleşmelere aşina olunmasını içerir.

2. Teknik bilgi: Hâkimlerin siber suçların teknolojik yönlerini kavraması gerekir. Bu, adli bilişim, ağlar, bilgisayar donanımları, kötü amaçlı yazılımlar, fidye yazılımları, kimlik avı, kripto para birimi ve karanlık ağ ve diğer siber suç araçları ve yöntemlerinin nasıl kullanıldığının anlaşılmasını içerir.

3. Dijital delillerin kullanılması: Eğitimler, dijital delillerin toplanması, korunması ve analizine ilişkin hukuki gerekliliklerin değerlendirilmesini kapsamalıdır. Bu, dijital deliller için gözetim zincirinin nasıl sürdürüleceğinin, adli bilişim uzmanlarıyla nasıl çalışılacağının ve bu tür delillerin mahkemede nasıl yorumlanacağının anlaşılmasını içerir. Bu aynı zamanda hassas materyallerin ele alınmasını ve savunmaya ifşa edilmesini de içerir.

4. Siber suç eğilimlerinin ve taktiklerinin anlaşılması: Teknolojinin hızlı gelişimi göz önüne alındığında, sürekli eğitimler, en son siber suç eğilimleri, taktikleri ve tehditlerinin yanı sıra bunlarla mücadele etmek için kullanılan araç ve stratejilere ilişkin güncellemeleri de içermelidir.

5. Uluslararası ve yargı bölgeleri arası sorunlar: Siber suçlar genellikle birden fazla yargı bölgesini kapsadığından, hâkimlerin uluslararası mevzuat ve suçluların iadesi anlaşmaları ve istinabe kuralları bağlamında diğer ülkelerdeki kamu makamlarıyla etkili bir şekilde nasıl iş birliği yapılacağı konusunda eğitime ihtiyaçları vardır.

6. Mağdur desteği: Siber suçların mağdurlar üzerinde önemli duygusal ve mali etkileri olabilir. Hâkimlerin mağdurlara nasıl etkili destek ve kaynak sağlayabilecekleri konusunda eğitim almaları gerekmektedir. Ayrıca hâkimler, özellikle mağdurun bir avukatının olmadığı durumlarda mağdura müdahil (katılan) haklarını açıklayabilecek şekilde eğitim görmelidir.

6. Adli Bilişim Uzmanları

a. Kabiliyetler

Adli Bilişim, elektronik cihazlarda depolanan verilerin belirlenmesi, elde edilmesi, işlenmesi, analiz edilmesi ve raporlanmasına odaklanan bir adli bilim dalıdır. Elektronik deliller, tüm cezai soruşturmalarda bir faktör haline gelmekte ve Türkiye'deki kolluk kuvvetleri, savcılar ve yargıya cezai soruşturmalar için destek sağlamaktadır.

Ortak Projenin İhtiyaç Değerlendirmesi kapsamında adli bilişim laboratuvarlarına ziyaretler gerçekleştirilmiştir. Ayrıca, adli bilişim laboratuvarlarından uzmanlar bazı çalıştaylara katılmıştır. Ekipman, süreç ve raporların incelenmesi sonucunda, Türkiye'nin, kolluk kuvvetleri ve savcıların kullanımına açık, profesyonel ve iyi donanımlı adli bilişim laboratuvarlarına sahip olduğu görülmüştür. Analiz uzmanları iyi eğitimlidir ve Türkiye'deki yetkili makamlarda istihdam edilen çok sayıda analiz uzmanı vardır.

Adli bilişim alanında karşılaşılan zorluklara ilişkin olarak yapılan bir değerlendirme, incelemenin kalitesinden ziyade analiz gerektiren cihazların niceliği ile ilgili sorunların olduğunu göstermiştir. Tartışılan bir diğer konu da savcıların adli bilişim laboratuvarına yaptıkları taleplerin standardıyla ilgiliydi. Savcılar inceleme için gereken detayları anlamıyor gibi görünmekte ve ne istendiği konusunda spesifik olmayan çok fazla talepte bulunmaktadırlar.

b. Delil materyallerinin ele alınması

Birçok durumda dijital cihazlar, hasar görmelerini veya ısı, nem, manyetizma veya uzaktan silme yoluyla veri kaybını önleyemeyen uygunsuz ambalajlarda laboratuvarlara gönderilmektedir. Bu da cihazların incelenemediği anlamına gelmektedir.

Bu soruna soruşturmada görev alan memurlar, savcılar ve diğer görevliler neden olsa da çözüm yöneticilerdedir. Doğru paketlemenin sağlanması şarttır. Bu esas, dijital cihazların uygun şekilde paketlenmediği sürece laboratuvarlara kabul edilmeyeceği yönündeki direktiflerle pekiştirilmelidir. Bu başlangıçta bazı ek gecikmelere yol açacak olsa da, zaman içinde herkes sisteme alışacak ve yönergelere uyacaktır.

Diğer sorunlar arasında, olay yeri incelemesi ya da davanın ilk aşamaları sırasında PIN kodu ya da şifresi alınmamış cihazların (cep telefonları) gönderilmesi yer almaktadır. Bu, analiz uzmanının veri elde etmek için kodu kırması gerektiği anlamına gelir (daha yüksek bir maliyetle) ve savcılar, olay yeri aramalarını ve delil materyallerinin sunulmasını yönetirken bunu göz önünde bulundurmalıdır.

c. Delil materyallerinin sunulması

Koordinasyon toplantılarına katılan adli bilişim temsilcileri, dijital cihazlar laboratuvara gönderilirken çok sık karşılaşılan başka sorunları da açıklamışlardır:

• Savcıların adli bilişim incelemesi için talepte bulundukları durumlarda, talep edilen şeyin kapsamının belirsiz olması ya da tanımlanmamış olması;

• Bu tür taleplerin soruşturulan suçun temel tanımını ve cihaza el koyma koşullarını genellikle içermemesi;

• Muğlak veya belirsiz olarak nitelendirilen taleplerin, talimatların net olmadığı durumlarda harcanan zaman nedeniyle genellikle ilgili Savcılık tarafından karşılanması gereken büyük maliyetlere yol açması;

• Analiz uzmanından bir yetişkine ait bir görüntünün uygunsuz olup olmadığı konusunda yorum yapmasının istendiği nesnel taleplerin sıklıkla sunulması. Bunlar bir adli bilişim analistinin eğitimini aşan öznel kararlardır.

Adalet Bakanlığı Adli Bilişim Laboratuvarı temsilcileri, bu delil materyali sunma hatalarının bazılarıyla başa çıkılabilmesi için laboratuvarın savcılara ve hâkimlere kurum içi eğitim vermesinin faydalı olacağını açıklamıştır. Tartışmaların birçoğunda Adli Bilişim ile ilgili konular ele alınmış ve bunlar Adalet Bakanlığı Adli Bilişim Laboratuvarından bir katılımcı tarafından dile getirilmiştir. Bu öneri olumlu karşılanmış ve bu raporda bir tavsiye olarak sunulmuştur.

Delil materyallerinin Adli Bilişim Laboratuvarına sunulması üzerine doldurulması gereken bir şablonun oluşturulması ve zorunlu olarak kullanılması önerilmektedir. Adalet Bakanlığı Adli Bilişim Laboratuvarı tarafından hazırlanması gereken bu şablonda dava detayları, el koyma detayları, referans numaraları,

kelime aramaları da dâhil olmak üzere laboratuvarda yapılması gereken ilgili detaylar yer almalıdır. Şifreler, PIN kodları, şüpheli ve tanık bilgileri gibi diğer veriler de şablona dâhil edilmelidir. Savcılar ve hâkimler iş gönderirken "neyin açık/belirgin bir görüntü teşkil ettiği" gibi tanımları da eklemelidir.

d. Analiz ve raporlama

Çalıştayların birçoğunda savcılar ve hâkimler kendilerine her zaman anlamadıkları adli bilişim raporları geldiğini ve bunların basitleştirilmesi gerektiğini belirtmişlerdir. Bu raporlar çoğu zaman, okunmalarını kolaylaştıracak bir terimler sözlüğü içermemektedir.

Adli bilişim birimlerinden temsilciler bu yorumları kabul etmiş ve bunları personele geri bildireceklerini belirtmişlerdir. Ancak mahkemelere gönderdikleri her rapora bir geri bildirim formu eklendiğini tespit etmişlerdir. Bu geri bildirim formlarının doldurulması ve/veya iade edilmesinin son derece nadir bir uygulama olduğu görülmüştür.

e. Çocuk Cinsel İstismar Materyali

Çalıştaylar sırasında, Çocuk Cinsel İstismar Materyali (ÇCİM) içeren dijital cihazların incelenmesi hakkında anlamlı konuşmalar yapılmıştır. Tartışmalarda, bu tür materyallerin diğer elektronik delillere benzer şekilde ele alındığı ve bunların ele alınması için özel bir usul bulunmadığı ortaya koyulmuştur.

ÇCİM'nin kopya sayısı asgari düzeyde tutulmalıdır. Örneğin, savcının analizde elde edilen video ya da fotoğrafların adli imaj ya da kopyalarına sahip olma zorunluluğu var mıdır? Ayrıca, sanık ya da müdafinin analizde elde edilen video ya da fotoğrafların adli imaj ya da kopyalarına sahip olmasına gerek var mıdır? Uluslararası en iyi uygulamalar, bu tür materyallerin paylaşılmasından kaçınmayı amaçlamaktadır ve savcı veya müdafinin bu materyallere erişmesi gerekiyorsa, kontrollü bir şekilde görüntüleme için adli bilişim laboratuvarına gidebilirler.

Türkiye'de hâlihazırda, bir şüphelinin bilgisayarına el koyulup imajının alındığı durumlarda, bu işlem tamamlanır tamamlanmaz bilgisayarın şüpheliye iade edilmesinin öngörüldüğü bir mevzuat mevcuttur. Türkiye'deki bu nadir yasal düzenleme, ÇCİM'nin faile iade edilmesine olanak tanımaktadır ki bu, materyalin nasıl ele alınması gerektiği ile karşılaştırıldığında kötü bir uygulamadır. Türkiye, Çocukların Cinsel Suistimal ve Cinsel İstismara Karşı Korunmasına İlişkin Avrupa Konseyi Lanzarote Sözleşmesini[21] imzalamıştır. Bu durum, çocukların mağduriyetten korunmasına ilişkin olarak sözleşmede yer alan bazı önemli ifadelerle çelişmektedir.

[21] https://www.coe.int/en/web/children/lanzarote-convention

7. Kamu-Özel Sektör İş Birliği

a. Siber suçlarla mücadelede kamu kurumları ve özel kuruluşlar arasındaki iş birliğinin önemi

Çalıştaylar, adli makamlar ile kamu kurumları/özel kuruluşlar arasındaki iş birliğinin siber suçlarda objektif suç unsurlarına ulaşmak ve bunları açıklamak için hayati önem taşıdığını ortaya koymuş ve aşağıdaki gibi birkaç kilit unsur belirlenmiştir:

1. Dijitalleşme ve özel mülkiyet: İnternet ve dijitalleşmenin karmaşık yapısı, zorunlu bir sektörel uzmanlaşmaya yol açmaktadır. Dolayısıyla, adli makamlar farklı türlerde dijital deliller toplamak için çeşitli sektörlerdeki farklı kuruluşlara ulaşmalıdır. Ayrıca, dijital teknolojilerin özel mülkiyeti, adli makamların IP adresi, banka hesap kayıtları gibi kişisel verilere doğrudan erişimini engellemektedir. Bu nedenle, siber suçların etkili bir şekilde önlenmesi ve bunlarla mücadele edilmesi için adli makamlar ile kamu kurumları/özel kuruluşlar arasında bilgi paylaşımı ve iş birliği bir gereklilik haline gelmektedir.

2. Sınır-ötesi delil toplama: İnternet, merkezi bir otorite olmaksızın fiziksel sınırları ortadan kaldıran dünya çapında bir olgudur. Milyonlarca kullanıcısı olan dijital hizmetler, farklı yargı bölgelerinde bulunan özel aktörler tarafından sağlanabilmekte ve siber suçlular bu hizmetleri sınır ötesi nitelikteki yasa dışı faaliyetleri için kullanmaktadır. Dolayısıyla, yabancı özel aktörlerden delil toplama uygulamaları siber suçlarla mücadele açısından çok önemli hale gelmektedir.

3. Uluslararası ve dijital para transferi: İnternet geleneksel bankacılık sistemini değiştirmiştir ve günümüzde insanlar ulusal sınırlardan bağımsız olarak paralarını herhangi bir banka şubesine serbestçe transfer edebilmektedir. Buna paralel olarak, banka kayıtları olmadan nakit akışını takip etmek neredeyse imkânsızdır. Adli makamlar, davalarını çözmek için "parayı takip et" ilkesine paralel olarak siber suçlulara ait banka hesaplarının kayıtlarını almak için adli müzekkere göndermelidir.

b. Türkiye'de siber suçlarla ilgili kamu-özel sektör ortaklıklarında yaşanan sorunlara örnekler

Türkiye'de kamu-özel sektör ortaklıklarında tespit edilen sorunlar aşağıdaki gibi özetlenebilir:

Hızlı teknolojik gelişmeler ve kapasite geliştirme ihtiyacı: Dijital alan hızla gelişmekte ve siber suçlular bu yeni teknikleri suç işlemek için kullanabilmektedir ve tüm özel aktörler bu gelişmeleri yakından ve yeterli teknik kapasiteyle takip edememektedir. Dolayısıyla, özel aktörler arasındaki teknik ve organizasyonel kabiliyet farklılıklarının siber suçlarla mücadele konusunda uyumlu bir işleyiş olasılığını engellediği görülmektedir. Bankacılık sektörü gibi yüksek düzeyde düzenlemeye tabi bir sektörde bile bankalar benzer düzeyde kaynak, araç veya yöntemlere sahip değildir ve bu da siber suçları önlemedeki başarıları ile adli makamlardan gelen iş birliği taleplerine verdikleri yanıtlar arasında farklılaşmaya neden olmaktadır.

İletişimsizlik ve veri paylaşımında gecikmeler: Adli müzekkerelerle ilgili olarak özel işletmelerden ve hizmet sağlayıcılardan düzenli gecikmeler yaşandığı ve bazen hiç yanıt verilmediği gözlemlenmiştir. Öte yandan, bu sorunun adli makamların usuller konusundaki bilgi eksikliğinden kaynaklanabileceği de belirtilmiştir. Bu bağlamda, talepler genellikle bankalar yerine ilgisiz taraflara veya Türkiye Bankalar Birliği ve BDDK gibi çatı kuruluşlara gönderilmekte (mevcut hukuki çerçevede her ikisinin de bu tür taleplere yanıt verme konusunda yasal yetkisi bulunmamaktadır) ve bu durum soruşturmaların uzamasına neden olmaktadır. Bu bağlamda, her sektörde bir çatı kuruluş oluşturulamasa bile, taraflar arasındaki iş birliği sistemi açık usul kuralları ve yönlendirmelerle optimize edilmelidir.

Sosyal medya platformlarının, dolandırıcılık faaliyetleri için kullanılan ve ele geçirilen hesapları devre dışı bırakma ve silme konusunda hızlı hareket etmediği de gözlemlenmektedir. Savcılıklar ve ilgili sosyal medya şirketlerinin temsilcilikleri arasında doğrudan bir iletişim sistemi kurulması da önerilmektedir.

Sosyal medya platformları: Büyük sosyal medya şirketlerinin merkezlerinin yurt dışında olması ve Türkiye ile sosyal medya şirketlerinin bulunduğu üçüncü ülkeler arasındaki maddi hukuk farklılıkları iş birliğinin başarı düzeyini engellemektedir. 5651 sayılı Kanun ve ilgili hükümleri bu şirketler üzerinde gerekli icrayı etkin bir şekilde sağlayamamaktadır. Budapeşte Sözleşmesi gibi uluslararası hukuki iş birliği mekanizmalarının daha etkin kullanılması, bu şirketlerle daha iyi ortaklıklar kurulması ve bu konuda daha etkin bir hukuki çerçeve düzenlenmesi, sınır ötesi dijital delillerin toplanması açısından büyük önem taşımaktadır.

Suç gelirlerinin takibi ve dondurulmasına ilişkin mevzuat: Bankacılık Kanunu ve BDDK'nin 61. maddesi ve uygulamasının da hileli işlem ve hesapların engellenmesinde etkin ve başarılı olmadığı görülmektedir. Bir yandan, yabancılar yeterli yasal kontroller veya doğrulama sistemi olmaksızın kolayca mobil hat alabilmektedir. Öte yandan, Türkler ve yabancılar e-para platformları, dijital ödeme hizmetleri, bahis siteleri ve kripto ticaret platformları gibi dijital platformlarda hesap açabilmekte ve yine uyumlulaştırılmış "müşterini tanı" (KYC) gereklilikleri olmaksızın kolayca para transferi yapabilmektedir. Bunlara paralel olarak, "patates hatlar" ve "para katırları" yargının gerçek siber suçluların yanı sıra önemli dijital delillere ulaşmasını da engellemektedir. Yabancılara mobil hat çıkarma koşullarının zorlaştırılması ve etkin kimlik doğrulama sistemlerinin dijital finans hizmetleri ve diğer ilgili dijital hizmetler (e-ticaret şirketleri, çevrim içi bahis siteleri vb.) için de kullanılması önerilmiştir.

8. Siber Suç Mağdurları

a. Siber suçların mağdurlar üzerindeki etkisine genel bakış

İçinde bulunduğumuz modern çağda teknoloji ve İnternet hayatımızın ayrılmaz bir parçası haline gelmiştir. Teknolojinin ve İnternet kullanımının ilerlemesiyle birlikte, siber suçlar hayatımızın her alanına dokunduğu için ciddi

bir endişe kaynağı olarak ortaya çıkmaktadır. Siber suç, suç faaliyetlerinin teknoloji ve İnternet kullanılarak gerçekleştirildiği karmaşık bir olgudur. Siber suçlar sanal bir alanda işlendiğinden düzenlenmeleri ve denetlenmeleri oldukça zordur. Siber suçların mağdurlar üzerindeki etkisi hem uzun süreli hem de sıkıntılı olabilmektedir.

Siber suçların ve siber ortam destekli suçların etkisi geniş kapsamlı olabilir ve genellikle mağdurlar için yıkıcı sonuçlara yol açabilirler. Siber suçların ve siber ortam destekli suçların mağdurlar üzerindeki etkilerinden bazıları aşağıda sıralanmıştır:

Duygusal hasar: Mağdurlar siber suçlardan duygusal olarak derinden etkilenebilir.

Siber suçlular mağdurların özel bilgilerini çalabilir ve bu durum mağdurların kendilerini çaresiz ve hakları ihlal edilmiş hissetmelerine neden olabilir. Mağdurların bir siber saldırının kendilerine verebileceği zararın farkında olmaları ve siber suçları önlemek için adımlar atabilmeleri çok önemlidir.

İtibari zarar: Siber suçlar nedeniyle mağdurların itibarına zarar gelebilir. Bu zarar genellikle mağdurların hayatında uzun süreli olur ve hızlı bir şekilde toparlanmayı zorlaştırabilir.

Mali kayıp: Siber suçlular genellikle kişilerin özel ve finansal bilgilerini çalar ve bunları mali kayba neden olacak şekilde kullanırlar. Bu tür suçların mağdurları gelecekte herhangi bir çevrim içi finansal faaliyete güvenme konusunda isteksiz hale gelebilirler.

Fizyolojik etki: Siber suçlar mağdurun ruh sağlığını ve iyi olma halini etkileyebilir.

Siber suç mağdurları kendilerini endişeli, depresif ve hakları ihlal edilmiş hissedebilirler. Bazı durumlarda, başlarına gelen bu olaydan dolayı utanç ve mahcubiyet de hissedebilirler.

Güvenlik sorunu: Siber suçlar nedeniyle mağdurlar güvenlik sorunları da yaşayabilirler. Bir mağdurun fiziksel konumuna siber suçlular tarafından erişilerek özel verileri ve bilgileri çalınabilir. Bu durum mağdurun hayatında sıkıntıya ve zihinsel baskıya yol açabilir.

Gizlilik tehdidi: Mağdurlar, siber suçlar nedeniyle önemli gizlilik tehditlerine maruz kalmakta ve bunun sonucunda kendilerini gizlilik konusunda güvensiz, hakları ihlal edilmiş ve depresif hissedebilmektedir.

b. Siber suç mağdurlarına destek ve kaynak sağlamanın önemi

Siber suçlar son zamanlarda giderek artan bir endişe kaynağı haline gelmiştir. Bu suçlar milyonlarca İnternet kullanıcısını etkileme kapasitesine sahiptir. Siber suçlar ve siber ortam destekli suçlar nedeniyle bir mağdur duygusal hasar, güvenlik sorunları, gizlilik tehdidi, psikolojik etki ve hukuki sonuçlara maruz kalabilir.

Bu gibi durumlarda mağdurlar güvenilir desteğe ve kendilerini destekleyecek uygun kaynaklara ihtiyaç duyarlar. Siber suçlular teknoloji meraklısıdır, dijital alandaki boşlukları bilirler ve bunları masum dijital kullanıcılara zarar vermek için kullanırlar.

Siber suçlar doğru stratejiler, devlet destekli adımlar, eğitim ve etkili kaynaklar kullanılarak engellenebilir. Siber suç mağdurlarının bu tür olumsuz durumlarla başa çıkmalarına yardımcı olmak için destek ve kaynaklar sağlanmalıdır. Bireylerin kendilerini bu tür siber tehditlerden korumak için proaktif adımlar atmaları da aynı derecede önemlidir. Bireylerin veya küçük/orta ölçekli işletmelerin bu tür suçlara karşı kendilerini güvende ve emniyette tutabilmeleri için kullanabilecekleri kaynaklar devlet tarafından sağlanmalıdır.

Çalıştaylarda siber suç vakalarının ihbar edilmemesinden, bir vakanın ihbar edilmesi üzerine mağdurlara nasıl davranıldığına kadar çeşitli konular gündeme gelmiştir.

İhbarda bulunulmaması: Siber suçların ihbar edilmemesiyle ilgili olarak, uluslararası alanda siber suçların eksik ihbar edilmesi sorununun önemli olduğu belirtilmiştir. Siber suç olaylarının %1'inden daha azının kolluk kuvvetlerine bildirildiği ve bunların da %1'inden daha azının ceza yargılaması kararıyla sonuçlandığı düşünüldüğünde, mahkûmiyetle sonuçlanan siber suç oranı oldukça düşüktür. Bu durumun ele alınması ve iyileştirilmesi zorunludur, aksi takdirde ceza adaleti müdahalesinin bu tür suçlar karşısında önemsiz hale gelme riski söz konusu olacaktır.

İhbar edilen siber suç sayısının düşük olmasının dolandırılmaktan duyulan utanç, ceza adaleti sistemine duyulan güven eksikliği, davanın mahkemeye taşınması ve bir sonuca varılması için geçen sürenin uzunluğu ile ilgili olduğu öne sürülmüştür. Mağdurların siber suçları ihbar ettiklerinde genellikle duyarsız kalındığı da kabul edilmiştir.

Mağdurların siber suçları ve siber ortam destekli suçları nereye ihbar etmesi gerektiklerini bilmeyebilecekleri de öne sürülmüştür. Bunun nedeni, hazır bilgi sistemlerinde (İnternet siteleri gibi) genellikle yetersiz bilgi bulunmasıdır. Bu durum çoğu zaman mağdurların siber suçları ve siber ortam destekli suçları yanlış kuruma veya birime bildirmelerine, gecikmelere ve elektronik delillerin kaybolmasına neden olmaktadır. Halkı bilgilendirme yöntemlerinin iyileştirilmesi ve çevrim içi bir siber suç ihbar sisteminin oluşturulması yoluyla siber suçların ihbar edilmesinin kolaylaştırılması önerilmiştir.

Yetkisizlik kararı: Bu, mağdurun suçu ihbar etmesi ve ardından savcının, suçun söz konusu savcının yetki alanı dışında meydana gelmesi nedeniyle daha fazla soruşturulmayacağını belirtmesidir. Mağdurlar bu durumda kendilerini farklı savcılıklara yönlendirilmiş olarak bulabilmektedir. Bu konuyla ilgilenmek üzere yakın zamanda bir mevzuat çıkarıldığı ve suçun artık kişinin ikamet ettiği bölgede soruşturulacağı belirtilmiştir.

Farkındalık ve önleme kampanyaları: Para katırlarıyla ilgili olarak, halkı bilgilendirme kampanyalarının faydalı olacağı düşünülmüştür. Pek çok para katırı, İnternet üzerinden verilen ilanlara cevap verdikten sonra kendi hesapları üzerinden suç fonları alacak şekilde kandırılmıştır. Bunun nedeni, birçoğunun saf olması ve bu tür dolandırıcılıkların nasıl gerçekleştirildiğini halka duyuran kamu bilgilendirme farkındalık kampanyalarının bu tür suçlara karışmalarını önlemede başarılı olmamasıdır. Birleşik Krallık'ta öğrencilerin bu tür dolandırıcılık olaylarına karıştıklarının fark edilmesi üzerine üniversite kampüslerinde bir farkındalık kampanyası düzenlenmiştir.

Veri korumanın etkisi: Yayınlanan Interpol istatistiklerine göre işlenen siber dolandırıcılık suçlarının sayısı her geçen gün artmaktadır. Bulut bilişim araçlarının ve hizmetlerinin yaygın kullanımı, kişisel verilerin hukuka aykırı olarak elde edilmesi ve yayılması konusunda büyük sorunları beraberinde getirmektedir. Mağdurlar kişisel bilgilerinin önemi ve bu teknoloji çağında bilgilerinin nasıl korunması gerektiği konusunda genellikle yeterince bilinçli değildir. Toplantılar sırasında, gençleri ve ergenleri bilgilendirmek ve kişisel verilerini ve kendilerini çevrim içi ortamda nasıl koruyacaklarını onlara öğretmek için okullarda eğitim programları düzenlenmesi önerilmiştir.

Örneğin, Birleşik Krallık Hükümeti siber suçlarla ilgili olarak halkın erişimine açık birçok çevrim içi kaynak ve rehberlik sunmaktadır. Bu kaynakları kullanarak bir birey doğru bilgilere erişebilir ve çevrim içi ortamda güvende kalmak için ihtiyaç duyduğu yardımı alabilir. Bu kaynaklar aşağıdakileri içerir:

Ulusal Siber Güvenlik Merkezi: Ulusal Siber Güvenlik Merkezi, Birleşik Krallık hükümetinin siber güvenlik konusunda destek ve rehberlik sağlayan bir kurumudur. Bu kurum, siber suçları önlemeyi ve mağdurlara çok ihtiyaç duydukları yardımı sağlamayı amaçlamaktadır (www.ncsc.gov.uk).

Siber Farkındalık: Siber Farkındalık (Cyber Aware), Birleşik Krallık Hükümetinin düzenlendiği bir kampanyadır. Bu kampanya, bir bireyin dijital alanda nasıl güvende kalabileceği ve kendini siber suçlardan nasıl koruyabileceği konusunda rehberlik sağlar (www.ncsc.gov.uk).

"Action Fraud": "Action Fraud", Birleşik Krallık'ın siber suçlar için ulusal ihbar merkezidir. Siber suçlar gece ya da gündüz herhangi bir saatte buraya bildirilebilir. Action Fraud'un hizmeti, mağdurun hem siber suçu ihbar etmesini hem de yardım ve desteğe erişmesini sağlar (https://www.actionfraud.police.uk).

Victim Support: Victim Support (Mağdur Desteği), Birleşik Krallık hükümeti tarafından kurulan bir hayır kurumudur. Bu hayır kurumu siber suç mağdurlarına destek sağlamaktadır. Ayrıca siber suç mağdurlarına gerekli destek ve rehberliği de sağlamaktadır (https://www.victimsupport.org.uk).

C. SONUÇLAR VE TAVSİYELER

Çalıştayda yapılan tartışmalar ve uluslararası uzmanlardan alınan bilgiler neticesinde aşağıdaki sonuç ve tavsiyeler belirlenmiştir:

1. Kolluk Kuvvetleri

1. Emniyet Genel Müdürlüğü ve Jandarmanın siber suçlarla ilgilenen birimlerinin bu alandaki deneyimlerini paylaşmaya teşvik edilmesine ihtiyaç duyulmaktadır.

2. Diğer ulusal birimlerle uyum sağlamak ve Türkiye'de siber suçlara yerel, bölgesel ve uluslararası düzeyde müdahaleyi koordine etmek üzere bir Ulusal Siber Suç Biriminin oluşturulması (bkz. paragraf 3a);

3. Çocuklara yönelik çevrim içi istismarla mücadeleye liderlik etmek ve Türkiye'de çocuk istismarına ve çocuk cinsel istismarı görüntülerine yönelik çevrim içi müdahaleyi yerel, bölgesel ve uluslararası düzeylerde koordine etmek üzere bir Ulusal Birimin oluşturulması (bkz. paragraf 3b);

4. Siber suçlar için çevrim içi ulusal ihbar merkezi rolünü yerine getiren özel bir merkezi ihbar sisteminin oluşturulması (bkz. paragraf 3c);

5. Kolluk kuvvetlerinin siber suçların soruşturulması ve elektronik delillerin ele alınması için özel bir eğitim stratejisi oluşturması ve uygulaması (bkz. paragraf 3d);

6. Soruşturma süreçlerinin kolaylaştırılması yoluyla kolluk kuvvetlerinin ve savcıların iş yükünün azaltılması. Müfettişler ve savcılar, delillerin toplanması ve/veya suçun ilişkilendirilmesi konusunda başarısız olması kaçınılmaz olan vakalarda soruşturma yürütmek yerine, kaynakları başarılı olması muhtemel soruşturmalara yönlendirmelidir (bkz. paragraf 3e).

7. Kurumlar arası iş birliği alanlarında acil iyileştirmeye ihtiyaç vardır. Avrupa Konseyi ve Türkiye ile görüşülen Kurumlar Arası İş Birliği Protokolünde detaylandırılan tavsiyelerin mümkün olduğunca çoğunun gözden geçirilmesi ve uygulanması tavsiye edilmektedir (bkz. paragraf 3f).

8. Türkiye'de gözetim, test amaçlı satın alma ve gizli operasyonlar gibi çevrim içi gizli soruşturma tedbirlerini yürütmek üzere özel kaynakların oluşturulması. İdeal olarak böyle bir birim Ulusal Siber Suçlar Birimi bünyesinde yer almalıdır, ancak böyle bir birimin oluşturulması zaman alacaktır. Bu kaynaklara kısa vadede ihtiyaç duyulmaktadır (bkz. paragraf 3g).

9. Kolluk kuvvetlerinin Türkiye genelinde siber suçlarla ilgili çeşitli farkındalık faaliyetleri ile koordineli ve anlamlı bir suç önleme planı uygulaması. Bu, mevcut Türkiye Ulusal Siber Güvenlik Stratejisinin gereklilikleri ile uyumludur (bkz. paragraf 3h).

10. Görevi Türkiye'de suç önleme planının uygulanmasına odaklanmak olan özel bir kolluk biriminin oluşturulması. İdeal olarak böyle bir birim Ulusal Siber Suçlar Birimi bünyesinde yer almalıdır, ancak böyle bir birimin oluşturulması zaman alacaktır. Bu kaynaklara kısa vadede ihtiyaç duyulmaktadır (bkz. paragraf 3h).

11. Emniyet Genel Müdürlüğü bünyesinde 7/24 görev yapan Tek İrtibat Noktasının ya da benzer şekilde eğitim almış görevlilerin, sosyal medya şirketleri ve çok uluslu hizmet sağlayıcılardan elde edilen elektronik delillerin nasıl korunabileceği ve delil olarak nasıl kullanılabileceği konusunda Türkiye genelinde savcılara ve yargıya eğitim ve farkındalık sağlanması. Bu eğitim, mütekabiliyet konusunda farkındalığı ve bazı hakaret davaları için materyal talep etmenin anlamsızlığına ilişkin açıklamaları içermelidir (bkz. paragraf 3g).

12. Siber suç mağdurlarıyla hassas bir şekilde ilgilenecek özel eğitimli polislere ihtiyaç vardır. Bazen bu faaliyetlerin cinsiyete özel olarak yürütülmesi de gerekebilir.

2. Savcılar ve Hâkimler

13. Ülke içindeki farklı yargı alanlarında siber suçlarla ilgili soruşturmalar için merkezi bir dosya sistemi kurulmasının değerlendirilmesi ihtiyacı devam etmektedir.

14. Adalet Bakanlığından savcılara uluslararası bilgi paylaşımı talepleri de dâhil olmak üzere, birimler arasında daha hızlı iletişimi sağlamaya yönelik kılavuzların ve şablonların uygulanması ihtiyacı devam etmektedir.

15. Savcı ve hâkimlerin zaman ve enerjilerini karmaşık siber suç davalarına harcamaları için (kariyerle ilgili) teşvikler yaratılması ve bu alanda yetkili hâkim ve savcıların yetkilerinin değiştirilmesi oranının azaltılmasının sağlanması.

16. Savcı ve hâkimlerin terfilerine karar vermek için tamamlanan dava sayısını bir ölçüt olarak kullanmak yerine, siber suç davalarına ilişkin başka kriterler benimsenmelidir. Siber suç davalarının karmaşıklığı nedeniyle, bu davalar diğer davalara göre daha yüksek puanlanmalı veya derecelendirilmelidir.

17. Eğitim ihtiyaçları düzenli olarak gözden geçirilmeli ve siber suçlarla ilgili hizmet içi eğitim çalışmaları sürekli olarak yürütülmelidir. Siber suçlarla ilgili eğitimler, standart hizmet öncesi eğitim müfredatının ayrılmaz bir parçası olmalıdır. Savcılar ve hâkimler için kapsamlı bir eğitim stratejisi olmalıdır. Her hâkim ve savcı, siber suçlarla ilgili delil teşkil eden tüm konularla etkin bir şekilde ilgilenebilmelidir.

18. Savcıların adli bilişim uzmanlarına delil göndermeleri için bir şablon olmalıdır. Adalet Bakanlığı böyle bir şablon geliştirme sürecindedir.

19. Ulusal Yargı Ağı Bilişim Sistemi (UYAP) ekranından izlenebilecek güncel ve ilgili içtihatları içeren haftalık veya aylık bir bülten hazırlanmalıdır.

20. Mentorluk girişimleri (akranlar arası), özellikle yüksek personel değişimi bağlamında, yeni personele yardımcı olacağı için teşvik edilmelidir.

21. Siber suç istatistiklerinin toplanmasına ihtiyaç vardır. Sadece siber suçlara ilişkin değil aynı zamanda eğitim faaliyetlerine ilişkin de kapsamlı istatistiklere erişim sağlanmalıdır.

22. Asliye Ceza Mahkemeleri ve Ağır Ceza Mahkemelerinin yetki alanına giren tüm bilişim suçları tek bir ihtisas mahkemesi tarafından görülmeli ya da büyük şehirlerde siber suçlar konusunda ihtisaslaşmış Ağır Ceza Mahkemelerinin sadece siber suçları davalarına bakması sağlanmalı, böylece diğer suçların yarattığı yük ortadan kaldırılmalı ve gerçek bir ihtisaslaşma sağlanmalıdır.

23. Siber suçlarda uluslararası iş birliği konusunda bilgi eksikliği vardır. Örneğin, bazı savcı ve hâkimler Budapeşte Sözleşmesi mekanizmalarından haberdar değildir. Bu nedenle, 7/24 irtibat noktaları hakkında eğitimler düzenlenmelidir.

24. En iyi uygulamaların geliştirilmesi ve desteklenmesi için koordinasyon toplantılarına benzer toplantılar düzenli olarak yapılmalıdır. Savcılar, hâkimler, kolluk kuvvetleri, diğer ilgili kurumlar ve özel sektörden temsilciler bu toplantılara davet edilmelidir.

3. Kamu-Özel Sektör İş Birliği

25. Bankacılık, telekomünikasyon, dijital hizmetler gibi doğrudan ilgili sektörlerde siber suçlarla mücadele konusunda sektörel kapasite geliştirme çalışmaları yürütülmeli ve uyumlulaştırılmalıdır. Mümkünse adli makamlarla iş birliği yapabilecek çatı kuruluşların kurulması ve kullanılması düşünülmeli ve sektörel bazda kamu-özel sektör iş birliğine ilişkin açık ve etkili kurallar ve kılavuzlar sağlanmalıdır.

26. Kurumlar arası yazışmalarda elektronik belge yönetimi ve Kayıtlı Elektronik Posta (KEP) uygulama sistemi daha etkin bir şekilde kullanılmalıdır. GSM şirketlerinin temsilcileri ve özel bankalar da bu sisteme dâhil edilmelidir.

27. BDDK ve Bankacılık Kanununun 61. maddesi ve uygulaması, hileli işlem ve hesapların engellenmesinde etkinlik ve başarının sağlanması için yeniden değerlendirilmelidir. Savcılıklar ve bankalar usulü koruma önlemleriyle daha hızlı hareket edebilmelidir.

28. Şüphelilere ait IBAN ve hesap bilgileri yeterli koruma önlemleriyle UYAP üzerinden kolluk kuvvetleri, savcılıklar ve/veya mahkemelerin erişimine açılmalıdır.

29. GSM operatörlerinde yabancılara mobil hat çıkarma koşulları zorlaştırılmalı ve dijital finans hizmetleri ve tüm dijital finansal hizmetler (e-para, dijital ödeme vb.) ve diğer ilgili dijital hizmetler (e-ticaret şirketleri, çevrim içi bahis siteleri vb.) için de etkin kimlik doğrulama sistemleri kullanılmalıdır.

30. Budapeşte Sözleşmesi gibi uluslararası hukuki iş birliği mekanizmalarının daha etkin bir şekilde kullanılması, sosyal medya şirketleriyle daha iyi ortaklıklar kurulması ve daha etkin bir hukuki çerçevenin düzenlenmesi sınır ötesi dijital delillerin toplanması için çok önemlidir. İlgili bağlayıcı hukuk ve bağlayıcı olmayan hukuk mekanizmaları çok paydaşlı bir bakış açısıyla yeniden değerlendirilmelidir.

4. Adli Bilişim Uzmanları ve Mevzuat

31. Çocuk Cinsel İstismar Materyallerinin (ÇCİM) ele alınması ve ifşa edilmesi için özel usuller olmalıdır. Bu, bir şüphelinin bilgisayarına el koyulduğu ve imajının alındığı durumlarda, bu işlem tamamlanır tamamlanmaz bilgisayarın kendisine iade edilmesi gerektiğine dair mevcut yasal gerekliliğin ÇCİM vakalarında uygulanmaması gerektiği anlamına gelir.

32. Ceza Muhakemesi Kanununun çok daha kapsamlı hale getirilmesi için değiştirilmesine ihtiyaç vardır. Bulutta arama gibi güncel sorunları karşılayan, aynı zamanda teknolojik açıdan nötr bir yaklaşımla gelişmekte olan teknolojilerden delil elde edilmesini sağlayan bir düzenleme, gerekli tüm usulü güvenceleri de içerecek şekilde uygulamaya koyulmalıdır.

33. Özellikle çocukların cinsel istismarına ilişkin görüntüleri içeren dosyaların şüpheli veya sanığa teslim edilmesine ilişkin olarak Ceza Muhakemesi Kanununun 134. Maddesinde değişiklik yapılmalıdır. Bu durum, kripto para cüzdanları, ele geçirilmiş veriler ve çok daha fazlasını içeren dosyaların bu maddenin bir gereği olarak şüphelilere iade edilmesi gibi diğer hususları da etkilemektedir.

34. Ceza Muhakemesi Kanunu Madde 12/6, adli makamlar arasındaki yetki çatışmalarını sona erdirecek bir değişiklikle açıklığa kavuşturulmalıdır.

35. Kamuda ve özel sektörde siber olayların ihbar edilmesini zorunlu kılacak yasal düzenlemeler ve kapsayıcı bir siber güvenlik mevzuatı hazırlanmalıdır.

36. Kamu ve kolluk faaliyetlerinde kişisel verilerin işlenmesine ilişkin mevzuatın düzenlenerek siber suçlarla mücadelenin yasal dayanağının temel haklara saygılı bir şekilde güçlendirilmesine ihtiyaç vardır.

37. Fidye yazılımı kullanımı yeni ortaya çıkan bir siber suç olarak tanımlanmalıdır.

38. Çevrim içi çocuk tacizi (siber kölelik/çevrim içi istismar) yeni ortaya çıkan bir siber suç olarak tanımlanmalıdır.

39. Kamudaki ve özel sektördeki siber olayların ihbar edilmesini gerektirecek kapsayıcı bir siber güvenlik mevzuatı düzenlenmelidir.

40. Kamu ve kolluk faaliyetlerinde kişisel verilerin işlenmesine ilişkin mevzuatı düzenleyerek temel haklara saygılı bir şekilde siber suçlarla mücadeleye yasal dayanak sağlayan eksiksiz bir düzenlemeye ihtiyaç duyulmaktadır.

41. Avrupa Konseyi Siber Suç Sözleşmesinin (Budapeşte Sözleşmesi) 2. Protokolü imzalanmalı ve iç hukuka aktarılmalıdır.

5. Siber Suç Mağdurları

42. Siber suçlar ve mağdur olmamak için İnternette ve diğer dijital forumlarda bireylerin kendilerini nasıl koruyacağı konusunda kamu bilincini artırmak amacıyla Hükümet öncülüğünde gerçekleştirilecek girişimlere ihtiyaç duyulmaktadır.

43. Çocukları ve gençleri siber suç faaliyetlerinin kurbanı olmamaları konusunda eğitmek için Milli Eğitim Bakanlığı öncülüğünde farkındalık kampanyaları düzenlenmelidir. Çocuklara ayrıca siber etik konuları da öğretilmelidir. Okullarda zorbalık, siber zorbalık, cinsel içerikli şantaj ve çocuk cinsel istismar materyallerinin dolaşımının sonuçları hakkında farkındalık yaratmak ve bunları önlemek için önleme ve farkındalık kampanyaları düzenlenmelidir.

44. Halk, siber suçların nereye ve kime bildirilmesi gerektiğinin farkında olmalı, siber suçların bildirilmesi için tek durak noktasının oluşturulması düşünülmelidir.

45. Gerektiğinde ekranların kullanılmasına ve/veya mağdurların ifadelerinin videoya kaydedilmesine olanak tanıyarak mahkeme prosedürleri sırasında mağdurların ve tanıkların haklarının korunması. Bu, bildirim kısıtlamalarını ve/veya anonimlik emirlerini içerebilir.

46. Soruşturma aşamasından davanın sonuçlanmasına kadar mağdur ve tanıklarla etkileşim konusunda en iyi uygulamaların (örneğin mağdurun dava süreci boyunca bilgilendirilmesi) oluşturulması.

This Project is co-funded by the European Union and the Council of Europe.
Bu proje, Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmektedir.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Bu Rapor "Türkiye'de Ceza Adalet Sisteminin Güçlendirilmesi ve Avrupa İnsan Hakları Sözleşmesi İhlallerinin Önlenmesi için Yargı Mensuplarının Kapasitesinin Artırılması" Avrupa Birliği ve Avrupa Konseyi Ortak Projesi kapsamında hazırlanmıştır.

Bu Proje Avrupa Birliği ve Avrupa Konseyi tarafından birlikte finanse edilmekte, Avrupa Konseyi tarafından yürütülmektedir. Projenin yararlanıcı kurumları Türkiye Cumhuriyeti Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü ve Türkiye Adalet Akademisidir. Projenin sözleşme makamı Merkezi Finans ve İhale Birimidir.

Avrupa Konseyi, Avrupa kıtasının önde gelen insan hakları kuruluşudur. Kuruluş bünyesinde 46 üye devlet bulunmaktadır. Avrupa konseyi üye devletlerinin tamamı; insan hakları, demokrasi ve hukukun üstünlüğünün korunmasını teminat altına almak üzere tasarlanmış olan Avrupa İnsan Hakları Sözleşmesi'ni imzalamıştır. Avrupa İnsan Hakları Mahkemesi, Sözleşme'nin üye devletlerdeki uygulanmasını denetler.