DİJİTAL ÇAĞDA SUÇLA MÜCADELE: BİR AVRUPA SİBER-SUÇ MERKEZİNİN KURULMASI*

AVRUPA KOMİSYONU Brüksel, 28.3.2012
COM (2012) 140 final

(Çev.) Arş. Gör. İsa BAŞBÜYÜK**

1. GİRİŞ: SINIR TANIMAYAN BİR SUÇA AVRUPA'NIN TEPKİSİ

Internet toplumumuzun ve ekonomimizin ayrılmaz zorunlu bir parçası haline gelmiştir. Genç Avrupalıların yüzde 80'i gerek kendi aralarında gerekse de dünya ile olan iletişimlerini online sosyal ağlarla[1] gerçekleştirmekte ve küresel anlamda her yıl 8 trilyon dolar e-ticarette el değiştirmektedir[2]. Fakat git gide online hale gelen günlük ve ticari muameleler karşısında yükselme gösteren cezai eylemler, her gün dünya çapında bir milyondan fazla insanın siber-suç mağduru olmasına neden olmaktadır[3]. Online cezai eylemler, bir euro gibi küçük bir rakama çalıntı kredi kartlarının satılması, kimlik hırsızlığı ve çocukların cinsel istismarı, kurumlara ve alt yapılara karşı gerçekleştirilen ağır saldırılar şeklinde değişiklik göstermektedir.

---

* Komisyon Tarafından Konsey'e ve Avrupa Parlamentosu'na Sunulan Bildirim

** Dokuz Eylül Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı

1 Eurostat, İnternet Erişimi ve Kullanımı, 14 Aralık 2010.

2 McKinsey Global Enstitü, Internet Sorunları: Ağ refah, çalışma hayatı ve büyümedeki etkiyi ortadan kaldırıyor. 2011 Mayıs Raporu, Erişim 8 Şubat 2012.

3 Norton Siber-suç Raporu 2011, Symantec, 7 Eylül 2011, Erişim 6 Ocak 2012.

Siber-suçların topluma maliyeti kayda değer miktardadır. Yakın tarihli raporlar siber-suç mağdurlarının dünya çapında her yıl 388 milyar dolar kaybettiğini, bu işin küresel çaptaki marihuana, kokain ve eroin ticaretinden daha karlı olduğunu ortaya koymaktadır[4]. Siber-suçların neye mal olduğuna ilişkin farklı yöntemler çeşitli maliyet hesaplarıyla sonuçlansa da, siber-suçların, bir taraftan yaygınlığı ve zararlı etkisi gittikçe artış gösteren diğer taraftan yüksek kazanç-düşük risk içeren bir yapıya sahip olduğu konusunda ortak bir kanı bulunmaktadır. Ekonomik büyümenin en üst seviyeye ulaştığı günümüzde, siber-suçlara karşı mücadelenin hızlandırılması, vatandaşların ve işletmelerin online iletişim ve ticaret güvenliğine olan inançlarının sürdürülmesi noktasında önem arz etmektedir. Bu mücadele aynı zamanda Avrupa 2020 stratejisi[5] ve Avrupa için Dijital Gündem'e[6] ilişkin büyüme hedeflerine katkı sağlayacaktır.

İnternet özgürlüğü son yılların dijital devrimini açıklamakta kilit rol oynamaktadır. Herkese açık olan Internet ne ulusal sınırlar ne de global bir yönetim kuruluşu tanımaktadır. Fakat bir taraftan internet serbestîsini Avrupa Temel Haklar Sözleşmesi doğrultusunda destekleyip korurken, diğer taraftan da bu serbestîden menfaat elde etmeyi amaçlayan organize suç örgütlerinden vatandaşı korumak için çaba göstermek zorundayız. Hiçbir suç yoktur ki, siber-suçlar gibi çıkarları ortak olan özel ve kamusal menfaat sahipleriyle birlikte emniyet güçlerinin koordinasyon halinde hareket etmesini ve sınırların ötesinde işbirlikçi yaklaşımı gerektirsin. Bu noktada AB önemli bir katkı sağlayabilir.

Avrupa Birliği siber-suçların önünü alabilmek için bir dizi girişimlerde bulunmuştur. Bunlar çocukların cinsel istismarı ve çocuk pornografisiyle mücadele için 2011 Direktifi ile 2012'de kabul edilmesi beklenen ve botnet'ler[7] başta olmak üzere siber-suç araçlarının kötüye kullanımının ceza-

---

4 Ibid.

5 Avrupa 2020 - Güçlü, sürdürülebilir ve kapsamlı bir büyüme stratejisi, COM(2010) 2020, 3 Mart 2010.

6 Avrupa İçin Dijital Gündem, COM(2010) 245 final, 26 Ağustos 2010.

7 Bilişim sistemlerine karşı saldırılara ilişkin Konsey ve Avrupa Parlamentosu Direktif Önerisi, COM (2010)517 final, 30 Eylül 2010. Botnetler, siber-saldırılara yönelik eylemleri yerine getirmek üzere uzaktan kontrol edilebilen, kötücül yazılımların bulaştığı tehlikeli bilgisayarlardan oluşan ağlardır.

landırılmasına yönelik bilgi sistemlerine karşı gerçekleştirilen saldırılara ilişkin Direktif'tir. Avrupa Polis Teşkilatı (Europol), çocuk seksi faili olduğu tahmin edilen 184 kişinin yakalandığı ve 200'ü aşkın çocuk istismarı mağdurunun tespit edildiği, bu yönüyle dünya çapındaki güvenlik güçleri tarafından yürütülen en büyük soruşturmalardan biri olan "Kurtarma Operasyonu"nda kilit rol üstlenerek, siber-suçlara yönelik faaliyetlerini arttırmıştır. Europol analizcilerinin, iletişim ağı merkezinde bir anahtar bilgisayar sunucusunun güvenlik özelliklerini çözümlemesindeki çalışmaları sayesinde, şüpheli faillerin kimlikleri ve eylemleri açığa çıkarılmıştır.

Başlıca yasal dayanak olan Siber-suç Sözleşmesi[8] çerçevesinde, siber-suçlarla mücadele öncelikli bir şekilde devam etmektedir. Bu, organize ve belirli ağırlıktaki uluslararası suçlara ilişkin olarak AB politika döngüsünde tanımlanmakta[9] ve siber güvenliği kuvvetlendirmek adına kapsamlı bir AB stratejisi geliştirmeye yönelik çabalarının ayrılmaz bütününü oluşturmaktadır. Avrupa birliği ayrıca siber güvenlik ve siber-suçlar konusunda süregelen AB-ABD çalışma gurubu örneğinde olduğu gibi, uluslararası partnerlerle de yakından ilişki kurmaktadır.

Belirtmek gerekir ki, siber-suçların Avrupa çapında etkili soruşturulması ve faillerin kovuşturulması aşamasında halen çeşitli engeller bulunmaktadır. Bunlar yargı yetkisi, istihbarat paylaşma imkânlarındaki yetersizlik, siber-suç faillerinin izinin sürülmesindeki teknik zorluklar, soruşturmaya ilişkin ve hukuki olanakların bir birine uymaması, uzman personel sayısındaki azlık, siber güvenlikten sorumlu diğer menfaat sahipleriyle işbirliği kurulmasının istikrara kavuşmaması şeklinde ifade edilebilir. AB aynı zamanda, İstikrar Aracı (IfS) kanalıyla, sınır aşan organize suçlarla mücadele için gerekli imkanlardan yoksun, gelişmekte yahut geçici nitelikte olan

---

[8] Avrupa Konseyi Siber-suç Sözleşmesi, Budapeşte, 23 Kasım 2001, Budapeşte Sözleşmesi olarak da bilinir. Sözleşme, ırkçılık ve yabancı düşmanlığı sergilemeye yönelik bilgisayar sistemleri aracılığıyla işlenen fiillerin suç olarak tanımlanmasına ilişkin Siber-suç Sözleşmesi ek protokolü içermektedir.

[9] AB politikasının, 2011-2013 yıllarına ilişkin olarak organize ve ciddi uluslararası suçlar konusunda sekiz önceliği bulunmaktadır; ki bunlardan birisi "organize suç grupları tarafından internetin kötüye kullanımın önlenmesi ve siber-suçlarla mücadelenin hızlandırılması"dır.

ülkelerdeki hızla yayılan ve uluslararası nitelik arz eden siber-suç tehdidine göndermede bulunmaktadır.

Söz konusu zorluklar karşısında, Komisyon İç güvenlik stratejisinin bir önceliği olarak, niyetinin Avrupa Siber-suç Merkezi kurulması yönünde olduğunu olduğuna işaret etmiştir[10]. Bu nitelikte bir merkezin kurulması hususunda yürütülen fizibilite çalışmalarına[11] dayanan Komisyon, Konsey'in talebi üzerine[12], Europol'a bağlı ve Avrupa Birliğinde siber-suçlara karşı verilen mücadelede odak noktası oluşturacak bir Avrupa Siber-suç Merkezi (EC3)'nin kurulmasını önermektedir. Fizibilite çalışmasından hareket eden bu bildiri, Avrupa Siber-suç Merkezi'nin temel fonksiyonlarını ana hatlarıyla belirterek; bu merkezin niçin Europol'a bağlı olarak kurulması gerektiğini ve nasıl kurulabileceğini açıklamaktadır. Fakat EC3 tam olarak çalışabilir konuma gelmeden önce, kaynak içeriği ayrı bir incelenmeyi ve hesaplanmayı gerektirecektir. Uygun görülmesi halinde bu merkezin kurulması, ileride Europol'un hukuki dayanaklarında revizyonu gündeme getirecektir.

2. AVRUPA SİBER-SUÇ MERKEZİ KURMA ÖNERİSİ

Avrupa Siber-suç Merkezi'nin artı bir değer oluşturabilmesi için, tamamlama ilkesine *(principle of subsidiarity)* saygı göstermek suretiyle, aşağıdaki temel siber-suç grupları üzerinde odaklanması önerilmektedir:

(i) Organize gruplar tarafından işlenen siber-suçlar, özellikle online dolandırıcılık gibi yüksek suç geliri sağlayanlar;

(ii) Çocukların cinsel istismarında olduğu gibi, internet üzerinden gerçekleştirilen ve mağdurları bakımından ciddi zarar meydana getiren siber-suçlar;

---

10 "2013 yılı itibariyle AB, bir taraftan uluslararası partnerlerle işbirliği kurma diğer taraftan soruşturmalara işlevsel ve analitik kapasite oluşturma konusunda muktedir olan Üye Devletler ve AB kuruluşları aracılığıyla bir siber-suç merkezi kuracaktır." AB Uluslararası Güvenlik Stratejisi işbaşında: Daha güvenli Avrupa için beş adım. COM (2010) 673 final, 22 Kasım 2010.

11 Bir Avrupa Siber-suç Merkezi için fizibilite çalışması, Nihai Rapor, Şubat 2012.

12 Siber-suçla mücadele için ortak bir strateji gerçekleştirmeyi konu olan bir Eylem Planına ilişkin Konsey Görüşü, 3010. Genel İşler Konseyi toplantısı, Lüksemburg, 26 Nisan 2010.

(iii) Birlikteki kritik öneme sahip altyapı ve bilgi sistemlerini etkilemeye yönelik (siber-saldırılar içeren) siber-suçlar[13].

Siber-suçların niteliklerinde gitgide yaşanan değişim göz önünde bulundurulursa, hem üye devletlerin gereksinimlerinin karşılanması hem de birliğin karşı karşıya kaldığı yeni siber tehditlerin üstesinden gelinmesine yönelik gerekli adımlar kapsam dâhilinde olmalıdır.

2.1. Temel Fonksiyonlar ve Bir Siber-suç Merkezinden Beklenenler

EC3 dört temel fonksiyon üstlenmelidir:

a) *Avrupa Siber-suçlar Bilgi Merkezi Fonksiyonu*

Bilgi toplama fonksiyonu, siber-suçlara ilişkin olarak özel yahut kamusal kaynaklardan beslenen ve mevcut polis verileriyle zenginleştirilen bir bilgi tabanını garanti altına alacaktır. Bu, siber-suçlarla mücadelede ve siber-güvenlikten sorumlu gruplardaki bilgi açığını aşama aşama doldurmalıdır. Toplanan bilgiler siber-suç faaliyetlerine, yöntemlerine ve sanıklarına ilişkin olacaktır. Söz konusu bilgiler bir taraftan siber-suçlar ile bu suçların önlenmesi, tespit edilmesi ve soruşturulmasına yönelik tecrübelerin geliştirilmesine hizmet edecek, diğer taraftan da Bilgisayar Acil Durum Müdahale Ekibi (CERT) topluluğu ve özel sektör Bilgi İletişim Teknolojisi (ICT) güvenlik uzmanları gibi icra makamları arasında uygun bir bağ oluşturulması noktasında destek sağlayacaktır. Bilgi paylaşımı gizlilik anlaşmalarına ve farklı taraflar arasındaki kurallara saygı duymayı gerektirmektedir.

Bilgi toplama işlevi aynı zamanda siber-suçların ihbarına ve bilgi paylaşımının gelişmesine katkı sağlayacaktır. Komisyon, ağır siber-suç saldırılarının ulusal emniyet güçlerine bildirilmesinin bir gereklilik haline getirilmesini üye devletlerden istemektedir[14]. Bu, ulusal polis servislerine ağır siber-suçlar konusunda EC3'e daha seri bir bilgi sağlama olanağı

---

[13] 8 Aralık 2008 tarih ve 2008/114/EC numaralı Direktifte tanımlanmıştır. Bu direktif şu an revizyona tabi tutulmaktadır, EC3 ileride meydana gelecek değişiklikleri dikkate alacaktır.

[14] Bilgi sistemlere karşı gerçekleştirilen saldırılara yönelik taslak direktifin 3 ila 7. maddelerinde listelenmiş türden olanlar, COM(2010)517 final, 30 Eylül 2010.

verecek; böyle EC3 söz konusu bilgileri yaymak suretiyle, bunların aynı amaca yönelik çalışan diğer üye devletlerdeki mevkidaşlarca bilmesini ve soruşturmalarda birbirlerinin bilgilerinden yararlanmasını mümkün hale getirecektir.

Amaç, eğilimleri ve tehditleri ortaya koyan yüksek kalitede stratejik raporlar üretmek; yaygın suç şekilleri konusunda bilinç oluşturmak ve çeşitli kaynaklardan beslenen bilgi tabanlı işlevsel bir istihbarat geliştirmek suretiyle, Avrupa'da siber-suç konusundaki bilgi tabanını genişletmektir.

b) *Üye Devletlere Kapasite Oluşumunda Destek Sağlamak İçin Avrupa Siber-suç Uzmanlarını Bir Araya Getirmek*

EC3 siber-suçların kontrol altına alınması için üye devletlere teknik bilgi ve eğitim konusunda yardımcı olmalıdır. Öncelikli hedef emniyet güçleridir, fakat eğitim desteğinin yargı mensuplarına da sunulması gerekmektedir. Daha iyi eşgüdüm ve bütünleyiciliğin sağlanmasına adına, Europol, Avrupa Polis Teşkilatı (CEPOL) ve üye devletlerin mevcut girişimleri düzene oturtulacaktır. Bu eğitim, siber-suç alanında başarı sağlamak adına polis memurları, savcılar, hakimler için derinlemesine teknik uzmanlık ile kapsamlı bir kapasite oluşturulmasına yönelik olmalıdır.

Siber saldırı olayları veya yeni online sahtekarlık şekilleri örneğinde olduğu gibi, üye devletlerden, uluslararası emniyet güçlerinden, yargı organlarından, özel sektör ve sivil toplum örgütlerinden gelen sorunlarla ilgilenmek ve bunları yanıtlamak; bilgi ve tecrübe aktarımını gerçekleştirmek üzere bir siber-suç masası oluşturulmalıdır.

Bu, Avrupa Birliği siber-suç çalışma koluna dâhil bulunan siber-suç konusunda uzman gruplar ile çocukların online cinsel istismarıyla mücadele uzmanlarının çalışmalarını desteklemeli ve onlara tavsiyelerde bulunmalıdır. Bu aynı zamanda gelişen siber-suç ağı uzmanlık merkezleri ile araştırma toplulukları arasında işbirliği oluşturmalıdır.

EC3 ayrıca siber-suçların online olarak rapor edilmesinin gelişmesi ve yaygınlaşması adına üye devletlerin göstermiş olduğu çabaları desteklemeli; çeşitli aktörlerden (şirketler, ulusal/hükümetsel CERT'ler, vatandaşlar vs.) ulusal emniyet güçlerine ve oradan da EC3 ulaşan bir rapor akışını temin

edecek bir bağlantı oluşturmak için, siber-suçların online ihbarını sağlayacak bir uygulama tertiplemelidir.

EC3, yargılama makamları ile kolluk üzerinden (deneyim, tecrübe) bilgi aktarımını kolaylaştıracak bir bağlantı oluşturmalıdır. Üye devletler nazarındaki ağır siber-suçların soruşturulmasında gelişme kaydedilebilmesi için, bu suçlarla mücadeleye adli makamların etkin katılımı büyük önem arz etmektedir.

c) *Siber-suçlara Yönelik Soruşturmalarda Üye Devletlere Destek Sağlamak*

Siber-suç Müşterek Soruşturma Ekipleri'nin oluşturulmasını sağlamak ve devam eden soruşturmalarda işlevsel bilgi alışverişinde bulunmak örneklerinde olduğu gibi EC3 siber-suçlara ilişkin soruşturmalara işlevsel destek sağlamalıdır.

Aynı zamanda siber-suç soruşturmaları için yüksek seviyede adli destek (tesis, yer ve araç) ve şifreleme uzmanı sağlamalıdır.

d) *Avrupa'daki Siber-suçların Soruşturulmasına İlişkin Kolluk ve Yargı Karşısında Ortak Bir Söylem Oluşturulması*

EC3 zamanla Avrupa'daki siber-suç soruşturmacılarını bir araya getirerek, bu soruşturmacılara daha iyi önlemin nasıl alınacağı ve araştırma faaliyetlerinde nasıl eşgüdümlü hareket edileceği konusunda, ICT endüstrisi ile diğer özel sektör kuruluşlarıyla (araştırma toplulukları, kullanıcıların dernekleri ve sivil toplum kuruluşları gibi) karşılıklı olarak müzakere edilmiş ortak bir düşünce oluşturma özelliğine sahip bir merkez olarak hareket edebilir.

EC3, İnterpol'ün siber-suçlara yönelik faaliyetleri ile diğer uluslararası siber-suç polis teşkilatları bakımından bir arabirim oluşturacaktır. Bu aynı zamanda internetin denetimine yönelik mevcut girişimlere ve BM hükümetler arası uzman guruplara veri aktarımını koordine edecektir.

EC3 aynı zamanda, ölçülü ve güvenli bir tutum sergilenmesini teşvik etmek amacıyla, Merkez analizleri tarafından yapılan siber-suç tanımla-

rındaki değişikliklere paralel olarak, INSAFE[15] gibi kamunun bilinçlenmesine rol üstlenen organizasyonlara güncel veriler sunarak, söz konusu organizasyonlarla sıkı iş birliği içerisinde olmalıdır.

2.2 Konum

Fizibilite çalışmalarındaki verilere göre, Avrupa Siber-suç Merkezi, Europol'un bir parçası olarak, onun mevcut yapısı içerisinde yer almalıdır.

Bu belirgin avantajlar. Europol üye devletler ile diğer menfaat sahipleri olan Interpol ve uluslararası kolluk yetkilileri arasında tanınmış bir konuma sahiptir; ayrıca bilgisayar suçlarını ele alma konusunda da yetki sahibidir[16]. Europol'un temel görevi, istihbarat analizi ve değişimi aracılı-ğıyla Avrupa kolluk makamlarına destekte bulunarak, bütün vatandaşların yararına güvenli bir Avrupa için çaba sarf etmektir.

2.3. EC3 Kaynak Gereksinimleri

Fizibilite çalışması çeşitli kaynak çıkarımlarını değerlendirmiştir. Bu çıkarımlar, özelikle gelecekte Europol tarafından verilmesi beklenen görevler ve AB mercilerinin personel istihdamı dikkate alındığında ilave bir değerlendirmeye ihtiyaç duyacaktır[17]. Bu değerlendirme bilhassa, Europol'un hukuki dayanaklarının revizyonu ve Komisyon'un İnternet Güvenliği Fonu önerisine yönelik halen sürmekte olan görüşme çerçevesinde tamamlanacaktır. Ancak gözüken o ki, bu hususta üye devletlerinde desteğine ihtiyaç duyulacaktır.

İhtiyaç duyulan kaynakların maliyet hesabı çıkarılırken, Komisyon üç sebep üzerinden hareket edecektir: Birincisi, siber-suçlardaki aşırı yükseliş karşısında, siber-suç dosya yükünde ölçülü bir artış olacağı düşünülmektedir. İkincisi, Üye devletler siber-suçlarla mücadelede mevcut kapasitelerini

---

15 Gençler için mobil cihaz ve internetten güvenli bir şekilde yararlanmayı teşvik eden Avrupalı Bilinçlendirme Merkezleri.

16 Avrupa Polis Merkezinin Kurulmasına ilişkin 6 Nisan 2009 tarihli Konsey Kararı (2009/371/JHA), ek ile birlikte madde 4 (1).

17 Değerlendirme, 2013 bütçesindeki faaliyetler için bütün istihdam ve bütçe ihtiyaçları ile çok yıllı finansal çerçevenin tutarlı olmasını gerektirmektedir.

arttıracaktır. Nihayet üçüncüsü, EC3 yalnızca belirli bir takım siber-suçları konusunda faaliyet gösterecektir.

2.4. İdare

EC3'ün, Europol'un bünyesinde yer alması, Merkezin stratejik yönetimine diğer önemli menfaat sahiplerinin katılımını sağlamak noktasında önem gösterecektir. Bu nedenle, Komisyon, başkanlığı EC3 tarafından yürütülen Europol'ün idari teşkilatı içerisinde bir EC3 Programı Kurulu oluşturulmasını önermektedir. Bu yapı, AB Siber-suçlar Müdahale Komitesi, ENISA ve Komisyon tarafından temsil edilen Eurojust, CEPOL, Üye Devletler gibi diğer menfaat sahiplerine, ek bir idari külfet altına girmeden kendi teknik bilgilerini kazanma imkânı verecektir. Kurul, EC3'ün siber-suçlara yönelik faaliyetleri yerine getirmesinden doğan sorumluluğun işletilmesi için harekete geçebilecek ve böylece, uzmanlığın kabul görmesi ve bütün menfaat sahiplerinin yetkilerine saygı gösterilmesi suretiyle onların ortak bir şekilde hareket etmelerini sağlayacaktır.

2.5. Önemli Aktörlerle İşbirliği

EC3 yalnızca AB kuruluşlarının ortak çalışmasını etkin kılmakla kalmayıp, aynı zamanda bu alanda tek bir başvuru noktası olarak hizmet sunan siber-suçlara karşı eşgüdümlü bir hareket alanı oluşturmalıdır.

(a) *Üye Devletler*

Temel amaç, siber-suçla mücadelede üye devletlere yardımda bulunmaktır. EC3 siber-suç yardım masası ve daha detaylı tehdit analizi ile daha fazla bilgi içeren işlevsel destek temini Avrupa çapındaki siber-suç araştırmalarına yararlı olacaktır. AB Siber-suç Komitesi, üye devletlerin meselelerinin EC3 Yönetim Programında ortaya konulmasını sağlayacaktır. Bunun dışında, üye devletler EC3 ile etkileşim için yeterli ara-yüzlere sahip olmak için, siber-suçla mücadele konusunda kendi ulusal yapısı içerisinde gerekli araştırmaların sürdürülmesine ihtiyaç duyacaktır.

(b) *Avrupa Kuruluşları ve Diğer Aktörler*

İlgili kuruluşlar, başta Eurojust, CEPOL ve ENISA'ya ilaveten CERT-EU olmak üzere, yalnızca yönetim programına katılmak suretiyle değil, aynı zamanda kendi yetkilerinin göz önünde bulundurulduğu etkili bir işbirliği yoluyla doğrudan EC3'ün faaliyetleri içerisinde yer alacaktır.

(c) *Uluslararası Partnerler*

Avrupa'da siber-suçlara ilişkin bilgi merkezinin oluşabilmesi için, EC3 siber-suçlar konusunda uluslararası partnerler bakımından önemli bir muhatap halini almalıdır. EC3, Interpol ve dünya çapındaki stratejik diğer partnerlerimizin işbirliğinde, siber-suçla mücadelede ortak bir hareket noktası oluşturulması için çaba sarf etmeli ve gelişen siber dünyada emniyet güçlerinin kaygılarının göz önünde bulundurulmasını sağlamalıdır.

(d) *Özel sektör, Araştırma Toplulukları ve Sivil Toplum Kuruluşları*

Siber-suçlarla mücadelede özel sektörle kolluk güçleri arasında güven ilişkisinin kurulması hayati öneme sahiptir. EC3, Europol'ün mevcut ve gelecekteki partnerleriyle bir arada çalışmasını temin etmek adına, iş çevresi ve diğer aktörler (araştırma toplulukları ile sivil toplum kuruluşları gibi) arasında güvenilir bir iletişim ağı ve bilgi aktarımını gerçekleştirecek bir yapı oluşturmalıdır. Bunlar, siber saldırılara karşı erken uyarıyı kapsayan toplumlar arası biz dizi hususların paylaşımına ve siber saldırı ile diğer siber-suçlara karşılık olarak işbirlikçi bir "müdahale ekibi" oluşturulmasına imkân sağlamalıdır.

EC3, hem siber-suçlara karşı mücadele etmek ve etkili koruma gerçekleştirmek hem de gelişen teknolojide zayıf noktaları minimize etmek amacıyla banka ve online satış firmaları gibi sanal mal varlığına sahip özel sektörün çabalarına da katkı sağlamalıdır.

Bir yandan siber-suç manzarasını ortaya koyan gerçek zamanlı daha iyi bir ölçüme ulaşmak diğer yandan geliştirilmiş yeni algılama yöntemleriyle siber-suç şebekelerinin ortadan kaldırılması ve siber-suçluların hızlı bir şekilde yakalanması için etkili bir çaba göstermek hem kolluk güçlerinin hem de özel sektörün karşılıklı menfaatinin oluşturmaktadır.

3. AVRUPA SİBER-SUÇ MERKEZİNİN UYGULAMAYA GEÇMESİNE YÖNELİK BİR YOL HARİTASI

3.1. 2013 Sonuna Kadarki Faaliyetler

Komisyon, Europol'le ortak temasta bulunarak içinde bulunduğumuz AB finansal çerçevenin sonuna kadar EC3'ün hayata geçirilmesinde başlangıç aşaması için ne kadar finans ve insan kaynağına ihtiyaç duyulacağını açıklayacaktır. Uygulama ekibinin görevleri, örnek olarak, EC3'ün görev tanımının, kurumsal yapısının ve performansın değerlendirmesine esas alınacak ilerleme kayıtlarının hazırlanmasını içerecektir. Düzenleme kurulunun rolü ve işleyişi ileriki aşamada ilgili menfaat sahipleri tarafından tanımlanacak ve onaylanacaktır.

Detaylı bir bilgi toplama işlevi oluşturulması amacıyla, EC3 uygulama ekibi hem CERT-AB ön düzenleme ekibiyle, hem de ilgili olduğu ölçüde ENISA ile bağlantı kurmalıdır (sınırlı kaynaklarını göz önünde bulundurmak suretiyle). Siber-suçların bildirimlerinde ilerleme kaydetmek adına, üye devletlerdeki mevcut online siber-suç bildirim sistemlerinin bir arada uyumlu şekilde çalışabileceği bir düzen kurmaya yönelik planlama çalışmaları yürütülecektir.

Bir siber-suç masası oluşturulmalıdır. Bu masa, özgülenmiş güvenli bir online topluluk platformu hükmüyle desteklenebilir. Europol, CEPOL ve Avrupa Siber-suç Eğitim ve Öğretim Grubu'nun mevcut eğitim çalışmaları değerlendirmeye tabi tutulabilir ve bu çalışmalara EC3 ile onun Düzenleme Kurulunun işbirliği çerçevesinde yön verilebilir. Hakim ve savcıların ihtiyaçlarına da cevap veren eğitim gereksinimlerine ilişkin bir analiz yapılmalıdır. Böylece ceza yargılaması sistemi mensuplarına açık, temel bir siber-suç eğitim programı ortaya konulabilir.

Ayrıca, gelecek Çok Yıllı Mali Çerçeve kapsamında alınan kararlar dâhilinde, gerekli finans ve insan kaynağına ilişkin olarak daha ayrıntılı bir değerlendirme yapılacaktır. Bu değerlendirme EC3'ün gelecekte kaydedeceği ilerleme hakkında bilgi sağlayacaktır.

4. SONUÇ

Dünya çapındaki organize suçların siber-dünyadaki faaliyetlerini arttırması karşısında kolluk güçlerinin buna ayak uydurması şarttır. AB, işin doğası gereği herhangi bir sınır tanımaksızın, gün geçtikçe gelişme gösteren siber-suç tehdidiyle mücadelede üye devletlere ve kuruluşlara gerekli araçları sağlayabilir. Eğer gerekli insan ve finans kaynağı temin edilebilirse, Avrupa Siber-suç Merkezi, Avrupa'daki siber-suçla mücadelede merkez noktası olarak hareket edecek; böylece siber-suç olgusu karşısındaki farkındalığı Birlik çapında artırarak, cezai soruşturmaları destekleyip, AB geniş çaplı çözümleri teşvik edecektir. Böylelikle, Merkez hem herkese açık bir İnternetin ve meşru sanal ekonominin teminine hem de Avrupa vatandaşlarının ve işletmelerin korunmasına katkıda bulunabilecektir.

Konsey bu önerinin kabul edilmesine davet edilmekte ve Merkez'in gelişimine katkı sağlama noktasında diğer menfaat sahiplerinin yanı sıra Avrupa Parlamentosu teşvik edilmektedir.