HUKUK İŞLERİ VE ULUSLARARASI İLİŞKİLER KOMİSYONU

V. TOPLANTISI

ANKARA-2016

RAPOR

"Siber Suçlarla Mücadele,
Yasal Çerçevesin Geliştirilmesi ve Üye Ülkeler Arasında İşbirliği"

GİRİŞ

Bilgi teknolojilerinin etki ettiği küreselleşme ve buna bağlı olarak meydana gelen yeni sorunlar, her devlet ve her birey için temel bir mesele halini almaktadır. Bu nedenle bilgisayar ağlarının süren yakınlaşması, küreselleşmesi ve artan dijital ortam yeni değişikliklerin bilincinde olmayı gerektirmektedir. Teknolojinin gelişmesi yepyeni fırsatların kapısını açmakta ve bunun yanında da genişleyen suç kavramı bilişim alanına sirayet etmektedir. Bilgi teknolojilerine bağımlılık yaşamın neredeyse her alanında, her yıl artmakta ve siber alanla ve suçlarla ilgili sorunlar daha da küresel bir nitelik kazanmaktadır.

Sonuç olarak, siber güvenlik riskleri, bu yüzyılda bir takım ekonomik ve ulusal güvenlik sorunlarını ortaya çıkarmaktadır. Bu hızlı değişim ile beraber Siber Suç kavramı ülkelerin gündeminde kayda değer bir yer tutmaktadır.

Hukuk İşleri ve Uluslararası İlişkiler Komisyonu, teknolojik ilerlemelerin etkileri ve sonuçları ışığında 29 Nisan 2015 tarihinde Bişkek'te yapılan Dördüncü Toplantısı'nda TÜRKPA üye ülkelerinde siber suçlarla mücadele ve hukuki çerçeve sorununa, bu sürece yasama boyutu ile parlamento katkısı perspektifi ile ele almaya karar vermiştir.

Bu itibarla Komisyon'un 2016 yılı Mayıs ayında Ankara'daki Beşinci Toplantısı, Genel Kurul'un Eylül 2016'da Bişkek'teki Yedinci Genel Kurul Toplantısı'nda Rapor'un ve Tavsiye Kararı'nın görüşülmesi düşüncesiyle *"TÜRKPA Üye Ülkelerinde Siber Suçlarla Mücadele Yasal Çerçeve"* konusuna ayrılmıştır.

TÜRKPA ÜYE ÜLKELERİNDE SİBER SUÇLARLA MÜCADELE ve YASAMA

1. Yeni bilgi teknolojileriyle uzay ve zaman sıkıştırılmakta, bununla beraber bol miktarda küresel bilgiye ışık hızında erişim ve anlık bilgi alışverişi imkanı sağlanmaktadır. Dolayısıyla modern dünyada siber alan, pratikte herşeye ve herkese dokunmaktadır. Ancak karşılıklı bağlantılardaki bu genişlik, bir yerdeki sorunun başka bir yerdeki bilgisayarları etkileme potansiyelinin de olduğu ve teknolojik gelişmenin dinamizmiyle birlikte siber güvenlik ve siber suç endişelerini de beraberinde getirdiği anlamına gelmektedir.

2. Elektronik bilgi akışı ve ağları, neredeyse yaşamın her alanında kök salmıştır. Küresel düzeyde birbirine bağlanmış bulunan iletişim altyapısı, günümüz faaliyetlerinin neredeyse hepsinde yer bulmakta ve ekonomi, sivil altyapı, kamu güvenliği ve ulusal güvenlik için kritik destek sağlamaktadır.

3. Diğer yandan, bilgisayar ve iletişim alanındaki gelişmeler, karmaşık siber güvenlik sorunlarından bazılarını öne çıkarır olmuştur. Daha gevşek düzenlenmiş dijital altyapının daha çok kişiye ulaşmasıyla birlikte birtakım açıklar daha fazla risk oluşturmaktadır. Siber saldırılar, maruz kalınan açıkları yıkıcı niteliklere dönüştürebilmekte ve ciddi sonuçlara yol açabilmektedir.

4. Ekonomiler ve ulusal güvenlik, bilgi teknolojisine ve bilgi altyapısına daha fazla bağımlı hale gelmektedir. Ağlardan oluşan bir yapı, ekonominin bütün sektörlerinin, başka bir deyişle enerji (elektrik gücü, petrol ve gaz), ulaştırma (demiryolu, havayolu, denizyolu),

finans ve bankacılık, bilgi ve telekomünikasyon, kamu sağlığı, acil durum hizmetleri, su, kimya, savunma, sanayi, gıda, tarım ve posta hizmetlerinin işleyişine destek olacaktır. Aynı zamanda bu yapılar elektrik transformatörlerini, boru hatları, radarları, v.s. de kontrol etmektedir.

5. Başta devlet organları olmak üzere, tüm kurum ve kuruluşların birçok hizmetlerini internet ortamında sunmaya başlamasıyla birlikte bu ortamda yaşanacak olumsuzluklar kişisel, sosyal ve ekonomik hayatı önemli ölçüde etkileme kapasitesine sahiptir. Oluşabilecek vakalar hem maddi hem de manevi zararları etkili olacaktır. Dolayısıyla bilgi ağlarına yapılan siber saldırılar, kritik faaliyetler üzerinde ciddi sonuçlara yol açabilmektedir. Günümüzde gittikçe artan bu riskler siber suçlara kapı aralamaktadır.

6. Siber suçlarla mücadele konusunda, çeşitli uluslararası örgütler ve kuruluşlar nezdinde, yine dünya çapında bir çok STK'nin inisiyatifiyle, aynı anda yürütülen birçok çalışmanın olması, sorunun hem ciddiyetini hem de bu konuya istenilen çözümün bulunulmasında ne kadar çok çaba sarf etmek gerektiğini göstermektedir. Bugüne kadar sağlanan gelişme kayda değer olmakla birlikte, siber suçla etkin bir mücadelede, henüz çok mesafe kat edilmesi gerektiği söylenmelidir.

7. Genel olarak yapılan çalışmalarda, siber suç kavramının bilişim teknolojilerinin gelişmesi ile ortaya çıkan veya bilişim teknolojilerinin kullanılması ile işlenen suçları ifade eden şemsiye bir kavram olarak kullanıldığı görülmektedir. Bunlar; doğrudan enformasyon teknolojilerini ve ürünlerini hedef alan, *(yetkisiz erişim, verilere veya bilgi sistemlerine zarar verilmesi vs.)* veya enformasyon/bilişim teknolojisi kullanılarak işlenen suçlar *(dolandırıcılık, kimlik kredi kartı vs.)* ve içerikle ilgili suçlar *(Çocuk pornografisi veya ırkçı içeriklerin yayınlanması veya bulundurulması suçları gibi)* olarak geniş bir alanda değerlendirilmektedir.

8. Uzun bir listeye sahip siber suçlarla mücadele hususunu ele alırken yenilikçi bir yaklaşım geliştirmek önemlidir. Siber suçlara ve siber terörizme karşı dijital cephenin yanısıra kişisel, toplumsal ve siyasi cephelerde de savaşılmalıdır.

9. Siber güvenlik ve suçlarla mücadele politikaları, tehditleri hafifletme, uluslararası katılımın, hızlı tepkinin, ve bilgisayar ağı işlemleri, bilgi güvenliği, hukuki yaptırımları gibi geniş bir yelpazeyi kapsamalıdır, zira bu konular küresel bilgi ve iletişim altyapısının güvenliğiyle ve istikrarıyla ilişkilidir.

10. Siber alandaki kırılganlıkları ele almak ve bilgi teknolojisi devriminin tam potansiyelinin küresel topluluk tarafından fark edilmesini sağlamak, hükümetlerin temel sorumluluğudur. Hükümetler, bir yandan ekonomik gereksinimleri ve ulusal güvenlik gerekliliklerini karşılarken diğer yandan da siber güvenlik açıklarıyla ve buna yönelik olarak çıkan suç ve ihlallerle mücadeleye yardımcı olacak araştırmalara daha fazla yatırım yapmalıdırlar. Tehditler ve riskler hakkında daha fazla toplumsal bilinç oluşturmak ve siber alan güvenliğine yönelik bütünleşik bir yaklaşım geliştirmek de önemlidir.

11. TÜRKPA üye devletleri, siber güvenlik ve suçlarla mücadelelerinde diğer birçok ülkede olduğu gibi tedbirler almaktadır. Bir yandan güvenliği, emniyeti ve gizlilik haklarını desteklerken diğer yandan da inovasyonu ve teknolojik gelişmeyi teşvik eden bir ortamı koruma paradoksuyla karşı karşıyadırlar.

12. Avrupa Konseyi "*Sanal Ortamda İşlenen Suçlar Sözleşmesi"ni* imzalayarak ratifikasyondan geçiren Türkiye'de konuyla ilgili olarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığınca "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" taslağı hazırlanmıştır. Bilgi Teknolojileri ve İletişim Kurumu ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve TÜBİTAK'ın işbirliğinde diğer Bakanlıkların da katılımıyla her yıl Ulusal Siber Güvenlik Tatbikatları yapılmaktadır. 2012 Temmuz ayında TÜBİTAK-BİLGEM bünyesinde "Siber Güvenlik Enstitüsü" kurulmuştur.

13. Türkiye'de bilişim ve internet ortamında işlenen suçlar ile ilgili mevcut mevzuat değerlendirildiğinde, 5237 sayılı "Türk Ceza Kanunu", 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", 5070 sayılı "Elektronik İmza Kanunu" gibi kanunlar ve ilgili yönetmeliklerle siber güvenlik hukuku altyapısının desteklendiği görülmektedir.

14. Azerbaycan Cumhuriyeti Avrupa Konseyi "*Sanal Ortamda İşlenen Suçlar Sözleşmesi"ni* (Budapeşte Konvensiyonu*) 30 Eylül 2009 yılında* ratifikasyondan geçirmiş ve Cumhurbaşkanı imzasıyla yürürlüğe girmiştir. Bunun yanında 1981 yılına ait Avrupa Konseyi Strasburg "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Hakkında Bireylerin Korunmasına İlişkin Sözleşme"ye taraf olmuş ve 209 sayılı kanunla kabul edilmiştir. Ayrıca "Elektronik İmza" ve "Devlet Sırrı" hakkında kanunlar bu alandaki önemli yasal çerçevelerdir.

15. Azerbaycan Ceza Kanununda doğrudan siber suç konusuna değinen maddeler vardır. (30. Bölüm, 271.,272.,273. Maddeler) Burada yetkisiz erişim, zararlı veri ve programların yayımı gibi konular üzerine hükümler yer almıştır. Yine aynı kanunda tahkir, hakaret ve haysiyeti yaralayıcı yayınlarla ilgili, internet ortamını da kapsayıcı şekilde düzenlenerek ceza hükümleri yer almıştır. (147 ve 148 Maddeler) Ayrıca Azerbaycan İdari Suçlar ile ilgili kanunun 16. Bölümü "Enformasyondan istifade edilmesi, yayımı ve korunmasına zarar veren kabahatler çerçevesinde, bilgilerin kullanımı, suistimali, dağıtımı ve korunması" hakkında maddeler içermektedir. Bunların yanında enformasyon teknolojilerinin kullanımında yaşanan ihlallere işaret eden diğer maddeler de kanunda yer almaktadır.

16. Kazakistan Cumhurbaşkanı tarafından imzalanarak 1 Ocak 2015 tarihi itibarı ile yürürlüğe giren Kazakistan Cumhuriyeti yeni Ceza Kanunu'nda, siber suçlar için getirilen cezai sorumluluklara ayrı bir yer verilmiştir. Bunlar; yetkisiz bilgisayar verilerine erişim, kanunsuz verilerin elde edilmesi, silinmesi ve değiştirilmesi, topluma zarar verme potansiyeline sahip, program ve verilerin yayılması şeklindedir. Ayrıca Ceza Kanunu çerçevesinde gerçek bir yenilikçi yaklaşım ile, bilgisayar ağları vasıtasıyla küçük düşürücü, aşağılayıcı ve iftira içeren nitelikteki bilgilerin yaygınlaştırılmasına yönelik

sorumluluklar artırılmıştır. Ayrıca hem BDT ülkeleri ile yapılan işbirliği neticesinde hazırlanan çalışmalar ve diğer uluslararası anlaşmalar çerçevesinde siber suçlarla mücadele faaliyetleri sürdürülmektedir.

17. Kırgız Cumhuriyeti Ceza Kanununda "Enformasyon teknolojileri alanında işlenen suçlar" hususunu doğrudan içeren üç madde yer almaktadır. (28. Bölüm). Yine Kırgız Cumhuriyeti İdari Sorumluluklar Kanunu çerçevesinde 21. Bölüm "Telekomünikasyon ağları ve iletişimin işletim ve kullanım kurallarını konu edinen ihlaller" adı altında düzenlenmiştir.

18. Günümüzün siber sorunlarla mücadelede sadece ulusal yasaların kabul edilmesi ve uygulanması yetersiz kalmaktadır. Siber suçlarla mücadele hakkında kalıcı yasaların ve yönetmeliklerin kabul edilmesi ve bunların gerektiği yerlerde ve zamanlarda tadil edilmesi gerekmektedir. Buna sebep olarak bilgi ve iletişim ağları, hem ulusal hem de uluslararası düzeyde büyük ölçüde özel sektörün mülkiyetindedir ve yine özel sektör tarafından işletilmekte olduğu gösterilebilir. Dolayısıyla siber güvenlik sorunlarının ele alınmasında, siber alanı güvence altına almaya katkıda bulunacak kamu – özel sektör ortaklığıyla birlikte uluslararası işbirliği ve normlar, geliştirilecek stratejilerin kilit unsuru olacaktır.

19. Siber ortamda yargılama yetkilerinin belirsizliği karşı karşıya kalınan bir sorundur. Normal şartlarda, her adli makamın yargılama yetkisi dâhilinde olan bölge coğrafi sınırlarla belirlenmiş durumdadır. İnternet ortamının sınır tanımayan küresel yapısı gereği, siber suçlar yargılama yetkileri birbirinden farklı alanlarla sınırlı olan pek çok adli makamı ilgilendirebilmektedir. Bu tür durumlarda, suçu oluşturan eylemleri hangi adli makamın soruşturacağı ve cezalandıracağı hususunda belirsizlikliğin giderilmesi önemlidir.

20. Parlamentolar, siber alan ve siber suçlarla mücadele konusunda kaygılarını seslerini duyurmaları ve sürdürülebilir kalkınmanın önemli bir vasıtası olarak siber güvenliği sağlamaya yönelik tedbirlerin artırılmasına daha fazla katkı yapmaları gerekmektedir.

21. Bir yandan muhtemel siber saldırılardan kaynaklanan zararları en aza indirirken ve hafifletirken diğer yandan da teknolojik kalkınmanın faydalarının yaygın bir biçimde anlaşılmasını ve desteklenmesini sağlamak amacıyla siber güvenlik ve siber suçlar alanında kapsamlı bir ulusal farkındalık oluşturacak şekilde mevcut hukuki mekanizmaları en yüksek düzeyde kullanmaları gerekmektedir.

22. Siber saldırılara ve müdahelelere karşı mücadelede ilgili kurumlara yeterince destek olabilmek için emniyet ve güvenlik kurumları ve adli sistem arasında karşılıklı etkileşimin ve koordinasyonun geliştirilmesine de özel bir önem verilmelidir.

23. Üye ülke parlamentoların, siber tehditlere ve siber suçlara karşı bütünleşik bir karşı eyleme geçilmesi için uluslararası bir strateji geliştirilmesine öncülük etmeleri ve bu itibarla ulusal ceza yasalarının uyumlu hale getirilmesi için ortak uluslararası hukuki mekanizmalar geliştirmelerine ihtiyaç vardır. Ayrıca işlenen fiilin, her bir ülkenin ceza

mevzuatında da suç olarak kabul edilmiş olması önemlidir. Ülke sınırları dışında bulunan herhangi bir suçlunun iadesi için, talep olunan ülkenin ceza mevzuatında da suç olarak kabul edilmiş olması (Doctrine of Dual Criminality) ve suçluların iadesine yönelik olarak kabul edilmiş olan bir anlaşmada fiilin suç olarak kabul edilmiş olması gerekmektedir.

24. En ileri teknolojilerin oluşturulması ve uygulanması suretiyle bilgi güvenliğinin güvence altına alınmasına yönelik pratik tedbirlerin eşgüdümlü bir biçimde uygulanması için özel sektörü desteklemek ve korumak amacıyla mevzuat geliştirilmesini desteklemek, yasama üyelerinin görevidir.

25. Siber güvenlik alanındaki yasaların uluslararası standartlarla hukuken uyumlu hale getirilmeye devam edilmesi önem arzetmektedir. Bununla beraber bilimsel ve teknolojik ilerleme temelinde sürdürülebilir kalkınmayla ilgili uluslararası akitlerin onaylanmasında da etkin bir rol üstlenmeleri ve bu hükümleri ulusal mevzuata aktarmaları da önemlidir.

26. Siber alanda koruma, gözetme ve yargılama yetkilerinin belirsizliği ile siber suçların pek çok ülke mevzuatında suç olarak tanımlanmasındaki belirsizlik nedeniyle siber saldırganların lehine oluşan güvenli sığınaklar, yurtdışından delil toplama ve suçluların iadesi gibi sorunları ortaya çıkarmaktadır.

Uluslararası Faaliyetler

Siber güvenlik, bilgi güvenliği ve ağ güvenliği konusunda yaşanan küresel sorunlar ve ortaya çıkan siber suçlarla ilgili olarak ancak temel paydaşları kapsayan uluslararası bir işbirliği stratejisi ve siber güvenlik kültürü ile ele alınabilir. Pek çok ülkeyi aynı anda etkileyebilen siber suçlarla mücadele edebilmek için uluslararası diyalog ve işbirliğine duyulan ihtiyaç yadsınamaz durumdadır.

27. Uluslararası siber suçlarla mücadele ile ilgili başlıca enstrümanlardan biri Avrupa Konseyi (AK) bünyesinde hazırlanarak 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan ve 1 Temmuz 2004 tarihinde yürürlüğe giren "*Sanal Ortamda İşlenen Suçlar Sözleşmesi"dir*. Bu Sözleşme/Konvansiyon, siber suçlarla mücadelede ulusal hukuki çerçevelerin nasıl uyumlu hale getirileceği ve uluslararası işbirliğinin unsurları hususunda rehberlik etmektedir. Bu hukuki akdin önemi, hem uygulamaya dönük hem de siyasidir. Sözleşme, siber suçlara karşı ulusal hukuki çerçeve geliştirilmesinin ana hatlarını ortaya koyduğu için bu konudaki Avrupa normları açısından önemli bir araçtır. Bunun yanısıra Sözleşme'nin imzalanması, siber suçluların sınırdışı edilmesi dahil operasyonel konularda uluslararası işbirliğini kolaylaştırmaktadır. Sözleşmenin siyasi önemi, siber güvenlik konusundaki tek bağlayıcı uluslararası sözleşme olmasıdır ve Sözleşme imzalanması da sözkonusu ülkenin kendi ulusal yasalarını siber suçlarla ciddi ölçüde mücadele edecek şekilde uyumlu hale getirmeye hazır olduğunu göstermektedir. Avrupa Konseyi, tüm dünyada Sözleşme/Konvansiyon'u desteklemek için özel sektörle ve üye devletlerle birlikte bir Küresel Proje başlatmıştır. Konvansiyon'a daha çok sayıda ülkenin katılıyor olması, kendi alanlarında sağladıkları kolaylıklarla siber saldırılara sponsorluk yapan suç grupları ve otoriteler için ciddi bir caydırıcılık unsuru oluşturmaktadır.

28. Avrupa Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) Bilgi Güvenliği ve Gizlilik Hükümetler Arası Çalışma Grubu (WPISP), bilgi toplumu ve direnç geliştirme politikaları hususunda tavsiye kararları ve raporlar hazırlamaktadır. Hükümet, iş dünyası ve sivil toplumdan uzmanlardan oluşan bir ağ üzerinden eğilimleri denetlemekte ve bilgi alışverişini kolaylaştırmaktadır. OECD, teknolojinin bilgi güvenliği ve gizlilik üzerindeki etkilerini analiz eden düzenli raporlar yayınlamaktadır.

29. Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT), bu konudaki görüşmelere 2008 yılında başlamıştır. O zamandan bu yana AGİT katılımcı devletleri, temel konular olarak ülkelerin siber suçlarla ve terörizmle mücadele kabiliyetlerinin geliştirilmesi ihtiyacının ve siber alanda sorumlu devlet tavrının belirlenmesinin ele alındığı birkaç üst düzey toplantı yapmışlardır. AGİT ülkelerinin, siber güvenlik konusuna yaklaşımlarında çok farklı ilgi alanları ve bakış açıları bulunmaktadır ve AGİT'in bu tartışmadaki tam rolünün ne olacağı hususunda tam bir uzlaşı oluşmamıştır.

30. BM Güvenlik Kurulu, önemli kararlar kabul etmiştir. BM Sosyal ve Ekonomik Komisyonu çerçevesinde 56/121 sayılı "Bilgi Teknolojisinin Suç Amaçlı Suistimaliyle Mücadele" ve 57/239 sayılı "Küresel Siber Güvenlik Kültürü Oluşturulması" kararları kabul edilmiştir. Her iki karar da uluslararası işbirliğinin önemini, siber suçlular için güvenli sığınakların ortadan kaldırılması, emniyet uygulamalarında işbirliği ve siber güvenlik konularında genel farkındalığın artırılması ihtiyacını vurgulamaktadır. "Küreselleşme ve karşılıklı bağımlılık: kalkınma için bilim ve teknoloji" hakkında 64/422 sayılı Karar, aynı zamanda BM ülkelerinin kendi siber güvenliklerini korumaya yönelik değerlendirme incelemesini de içermektedir. Bu girişimler, siber tehditler konusunda artan kaygılara dikkat çekmiş, küresel bir farkındalık oluşturmaya yardımcı olmuş ve BM ülkelerini siber güvenlik konusunda kendi ulusal mekanizmalarını ileriye taşımaları için gerekli tedbirleri almaya yöneltmiştir.

31. AB Komisyonu tarafından Mayıs 2007'de kimlik bilgileri hırsızlığına karşı "Siber suçlarla mücadele üzerine genel bir politikaya doğru" adıyla bir girişim başlatılmıştır. AB konuya birbiriyle örtüşen farklı temalarla paralel politikalar uygulamaya konulmuştur. "*Siber suçlarla mücadelede genel bir politikaya doğru"* adlı yayınlanan çalışma, operasyonel emniyet alanında işbirliğinin, siyasi işbirliğinin ve üye devletler arasında işbirliğinin geliştirilmesini öngörmektedir. Bununla birlikte muhtemel bir hukuki harekete yönelik olarak sektörde bilincin artırılması, eğitim, araştırma ve daha güçlü diyalogun yanısıra üçüncü ülkelerle siyasi ve hukuki işbirliğini de teşvik etmektedir. *"Karşı köktenleşme*" yani şiddet içeren ideolojik materyalleri denetleme kabiliyeti, uzun zamandır AB karşı terörizm stratejilerinin odak noktası olmuştur. Aralık 2009'da, Avrupa Birliği'nin "dahili güvenlik" gündeminde ciddi bir adım oluşturan "Stokholm Programı" kabul edilmiştir. Program, Avrupa Dahili Güvenlik Stratejisi çağrısında bulunmanın yanısıra daha iyi ve daha dirençli ağ bilgisi güvenlik tedbirleri geliştirme gereği, siber saldırılarla daha iyi mücadele kabiliyeti, bütün üyelerin Siber Suç Konvansiyonu'nu onaylamasının önemi ve hem hükümetler arasında hem de özel sektörle bilgi alışverişinin önemi dahil olmak üzere siber güvenliğe dair birtakım referanslarda bulunmaktadır. Ekim 2010'da kabul edilen yeni AB İnternet Güvenliği Stratejisi, Siber Alanda vatandaşların ve işletmelerin güvenlik seviyesini yükseltmeyi amaçlamakta ve siber suçlarla mücadeleyi hedeflemektedir. Stratejideki üç özel öneri arasında 2013 yılı itibarıyla AB Siber Suçlarla Mücadele Merkezi kurulması, 2012 yılı itibarıyla bütün AB kuruluşlarında Bilgisayar

Acil Durum Tepki Ekipleri (CERTS) Ağı kurulması (ve aynı zamanda bu kuruluşların emniyet güçleriyle işbirliği içine girmesi) ve 2013 yılı itibarıyla Avrupa Bilgi Paylaşımı ve Uyarı Sisteminin (EISAS) hayata geçirilmesi yer almaktadır. Konsey, emniyet güçlerine daha iyi sınır-ötesi eğitim sağlanması ve uluslararası düzeyde daha iyi koordinasyon için 2010 yılında Europol'un Avrupa Siber Suçlar Platformu'nun (ECCP) güçlendirilmesi çağrısında bulunan Siber Suçlar Eylem Planı'nı kabul etmiştir.

III. SONUÇLAR

- ✓ Günümüzde kişi, kurum ve kuruluşlara ait bilgi varlıklarının hacminin ve çeşitliliğinin geçmişe oranla ciddi artışlar gösterdiği açıktır. Artık bilgi varlıklarımızın çok büyük ölçüde sayısallaştığı ve bu durumunun gerek kamu gerekse özel iş süreçlerini kolaylaştırmaktadır. Geçmişte mümkün olmayan yeni hizmetleri mümkün hale getirmekte ancak bütün bunların yanı sıra, siber güvenliğin ve siber suçlarla mücadele konusunun ciddi bir sorun teşkil ettiğinin kabul edildiği ve gerekli eylemlerin ivedilikle hayata geçirilmesi gerektiği ortadadır.

- ✓ Siber alanda, ulusal sınırlar çok az anlam taşır. Siber alanın küresel niteliğinden ötürü mevcut zayıflıklar, dünyanın gözü önünde cereyan eder ve istismar etmek için yeterli kabiliyeti olan herkes tarafından heryerde ulaşılabilir. Siber ortamda saldırgan ve mağdurların çoğu durumda farklı ülkelerde yer alabildiği. dolayısıyla siber suçlarla mücadele ve güvenlik alanında, uluslararası birlikte çalışılabilirlik mekanizmalarının ve sözleşmelerin önem kazandığı. suç amaçlı suistimaliyle mücadele alanında devletler arasında daha *fazla koordinasyon ve işbirliği* gereksinimini öne çıkarmaları ve bu bağlamda uluslararası ve bölgesel örgütlerin oynayabileceği rolü vurgulamaları gerekir.

- ✓ Ülkeler bir yandan güvenliği, emniyeti ve gizlilik haklarını desteklerken diğer yandan da inovasyonu ve teknolojik gelişmeyi teşvik eden bir ortamı koruma paradoksuyla karşı karşıyadırlar. Siber güvenliğin emniyet altına alınması, hem ulusal hem de uluslararası düzeyde devletler, işletmeler ve toplum için temel bir sorundur.

- ✓ Siber ağlara yönelik olarak daha çok sayıda saldırı yapılıyor olması, güvenli, emniyetli ve dirençli bir siber ortam oluşturulması ve siber güvenlik bilgisinin ve yeniliklerin desteklenmesi için *yasal mevzuatın geliştirilmesi* sonucunu ortaya çıkarmaktadır. Uluslararası sözleşmelerin onaylanmasına müteakip iç hukuka uyarlanması sibersuçlara *karşı mücadelesinin sistemleştirilmesi açısından* önemli bir ihtiyaçtır.

- ✓ Gerekli mevzuatlar hazırlanırken kamu - özel sektör katılımı, kilit unsurudur. Kamu - özel sektör katılımı farkındalık, eğitim, teknolojik gelişim, zayıflıkların giderilmesi ve yenilenme faaliyetleri ele alınırken çeşitli biçimler alabilir.
- ✓ Siber güvenlik ve suçlarla mücadele, mevzuat çalışmalarında, hukukçu, teknik kişi, sosyolog-psikolog gibi sosyal bilimci vb. farklı disiplinlerinden oluşan mesleki uzmanların katkı vermesinin hukuki ve teknik altyapı uyumluluğunun sağlanması noktasında önem arz etmektedir.

- ✓ Ülkelerimizde siber güvenlik hukuku konusunda daha fazla uzman yetiştirilmesine ihtiyaç olduğu ve bu konuda üniversitelerin ve kurumların gerekli eğitim, sertifikasyon ve tez çalışmaları yapılmasına imkan sağlamasının daha çok faydalar getireceği ve sürecin sağlılık olarak yönetilmesine büyük katkılar sağlayacaktır. Kamu, özel ayrımı yapmadan ülke Kritik Altyapının korunması için hukuki ve teknik düzenlemelerin ayrıca ve ivedilikle ele alınması gerektiği; bu konuda yürütülecek bilimsel çalışmaların desteklenmesinin fayda sağlayacaktır.

- ✓ Küresel düzeyde siber suçlarla mücadelede siber güvenlik kültürünün teşvik edilmesi, desteklenmesi, geliştirilmesi ve kuvvetle uygulanması gerekir.

- ✓ TÜRKPA üye ülkeleri, siber suç ile mücadele için bir ortak yasal çerçeve üzerine çalışmalı bunun yanı sıra bilgi ağlarının korunması için müşterek bir faaliyetin geliştirilmesi adına yakın işbirliği yapmalı bu alanda taraf olunan uluslararası akitler incenmelidir.