BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

SEKTÖREL ARAŞTIRMA VE STRATEJİ GELİŞTİRME DAİRESİ BAŞKANLIĞI

DİJİTALLEŞEN DÜNYADA BİLİŞİM SUÇLARI VE MÜCADELE YÖNTEMLERİ

2022

Bu rapor, bilgilendirme amaçlı hazırlanmış olup, Bilgi Teknolojileri ve İletişim Kurumu'nun resmi görüşü olarak değerlendirilemez ve gösterilemez.

İÇİNDEKİLER

GİRİŞ

Bilişim kelimesi; "insanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi" olarak açıklanmaktadır. Bilişim; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerdir. Bilişim sistemi ise, 5237 sayılı TCK'nin 243. maddesinin gerekçesinde; verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemler olarak tanımlanmıştır. Avrupa Konseyi Siber Suç Sözleşmesi'nin "Tanımlar" başlıklı birinci maddesine göre ise Bilişim sistemi; bir veya birçok unsuru, bir programın işleyişi aracılığıyla verilerin otomatik olarak işleme tabi tutulmasını sağlayan, birbirine bağlanmış veya benzeşen tek veya toplu tertibatı ifade etmektedir. Bilişim sistemlerinin en yaygın unsuru, verilerin saklanması, işlenmesi ve aktarılmasını sağlaması bakımından bilgisayarlardır. Ancak bilgisayarlar dışında da bilişim sistemi olarak nitelendirilebilecek aygıtlar mevcuttur. Bu itibarla, bilişim suçu olarak isimlendirilen fiiller, bir bilgisayarda ya da bilgisayar olarak nitelendirilmemesine rağmen, veri iletişimi sağladığı için Bilişim alanına dahil unsurlardan sayılması gereken diğer elektronik, manyetik, mekanik araçlar üzerinde (örneğin, WAP uyumlu, girilen verileri saklayabilen, işleyebilen, aktarabilen cep telefonları ile üzerindeki WEB paneli sayesinde ağa bağlanıp veri aktarımı yapabilen elektronik ev aletleri) veya bunları veri iletişimi için birbirine bağlayan soyut veya somut ağlar üzerinde işlenebilmektedir.

Bilişim teknolojilerinin eğitimden ticarete, ulaşımdan iletişime, kamu hizmetlerinden özel sektöre kadar hemen her alanda köklü değişiklikler yaparak hayatı ciddi anlamda etkiler hale gelmesi, bilişim teknolojilerinin kanunları ihlal etme fırsatı veren ve ortaya yeni suç fiilleri çıkartan bir etkiye sahip olmasını da beraberinde getirmiştir. Bu sebeple, özellikle bu teknolojilerin kaynağını oluşturan ülkeler başta olmak üzere, pek çok devlet bilişim alanında yasal düzenlemelere gitmiş, mevzuatlarını teknolojinin gerektirdiği biçimde değiştirme çabasına girmişlerdir.

Kanun koyucular bu alandaki suçları karşılamak için mevzuatlarında ya ayrı özel bir kanun yapmakta, ya da mevcut ceza kanunları içinde düzenleme gerçekleştirmektedirler. Yeni Türk Ceza Kanunu (5237 Sayılı TCK)'nda ise, bu alandaki suçlar hem "Bilişim Alanında Suçlar"

adı altında bir bölümde düzenlenmiş, hem de hırsızlık, dolandırıcılık gibi suçlar içerisinde yer almışlardır.[1]

Bilim ve teknoloji alanındaki ilerlemeler, küreselleşme olgusunun beraberinde getirdiği gelişmelerle bir araya geldiğinde karşımıza çok daha farklı ve karmaşık bir güvenlik algısı çıkmaktadır.

Klasik güvenlik anlayışı, genel anlamda coğrafi sınırlar üzerinden askeri güç merkezli çıkarımlar yapmakta ve bu yönde bir güvenlik perspektifi oluşturmaktaydı. Ancak Soğuk Savaş'ın sona ermesi, iki kutuplu dünya düzeni üzerine kurgulanmış uluslararası sistemde değişime neden olmuştur. Çok kutuplu ve hegemon ABD'nin oluşturduğu yeni uluslararası sistemde devletlerin yanına çok uluslu şirketler, uluslararası kurum ve kuruluşlar gibi yeni aktörler eklenmiştir.

21. yüzyılda yaşanan bu gelişmeler ışığında güvenlik algısının çok boyutlu bir hal alması da kaçınılmaz olmuştur. Bu boyutlar arasında ekonomik, çevresel, siyasal ve sosyal boyutlar sayılabilir. Güvenlik konusunun farklı boyutlarda değerlendirilmesinin en önemli nedenlerinden biri de internetin günlük hayatın içerisine hızlı ve yoğun bir şekilde girmesidir.[2]

[1] YILMAZ Sacit, 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar, http://tbbdergisi.barobirlik.org.tr/m2011-92-669

[2] EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

1 BİLİŞİM (SİBER) SUÇLARI

İçinde bulunduğumuz 21. Yüzyılın "Bilgi Çağı" olarak nitelendirilmesinin yanında, bilgi alış verişinin saliselerle kısıtlanması insanoğlunun bilgiye olan açlığının yanı sıra yaşamını sürdürmesinin tek yolu olarak önümüze çıkmaktadır. Bu çerçevede bilişim teknolojileri insanı şaşırtan boyutlarda büyüyerek örümcek ağı gibi tüm dünyayı kaplamakta, hayatımızın her alanına nüfuz ederek durmaksızın geniş bir konsepte yayılmaktadır. Tarihsel gelişim evresi boyunca bilişim sektöründe meydana gelen marjinal faydası yüksek gelişmeler ve beraberinde getirdiği sorunlarla birlikte bilişim suçları ortaya çıkmıştır.[3]

Bilişim Suçu **en genel anlamıyla** bilişim alanındaki gelişmelere paralel artış gösteren ve teknolojinin yardımı ile genellikle sanal bir ortamda kişi veya kurumlara maddi veya manevi zarar verecek davranışlarda bulunmaktır. Başka bir tanım, bilişim sistemine yönelik veya bilişim sistemi kullanılarak işlenen suç olduğunu söylemektedir. Diğer bir tanımda ise "bir bilgisayarda ya da bilgisayar olarak nitelendirilememesine rağmen veri-iletişimi sağladığı için bilişim alanının unsurlarından olduğu kabul edilmesi gereken diğer elektronik, manyetik, mekanik araçlar üzerinde (örneğin, cep telefonları, üzerindeki web paneli sayesinde ağa bağlanıp bilgi aktarımı yapabilen elektronik ev aletleri, üzerinde yüklü programlar aracılığıyla şifreli yayınları alan, bunları işleyen ve bunlardan sonuç çıkaran dekoderler) veya bunları veri-iletişimi için birbirine bağlayan soyut veya somut bir ağ üzerinde gerçekleştirilebilir eylemler" bilişim suçu olarak nitelendirilmektedir. Ne var ki, doktrinde üzerinde uzlaşılmış bir Bilişim Suçu tanımı da tam olarak bulunmamaktadır. Bilişim ortamında işlenen suçları karşılamak için; Bilgisayarla (Kompüter) işlenen Suçlar, Bilgisayar Suçu/Suçları, Bilgisayarla ilgili Suç, Bilgisayar Suçluluğu, Bilişim İhlali, İnternet Suçları, Bilişim Suçları, Siber Uzay Suçları, İleri Teknoloji Suçu ve Çok Yargısal Suçlar gibi kavramlar kullanılmaktadır. Bu kavramlardaki çeşitlilik bütün ihlalleri tek bir kavram altında toplama ihtiyacını doğurmuştur.

Türkiye'nin üyesi olduğu Avrupa Konseyi Bilişim suçlarını nitelendirirken "Siber Suç" kavramını kullanmıştır. Uluslararası platformlarda da yoğunlukla yine Siber suçlar kavramı kullanılmaktadır. Bilişim suçu Türk Ceza Hukuku'na ilk kez 1991 yılında 3756 sayılı Kanun'la girmiştir.

[3] ALTUNOK Ebru, VURAL Ali Fatih, Bilişim Suçları, s.1, 2011/8
https://dergipark.org.tr/tr/download/article-file/208853

Mezkûr Kanun,

1) Sistemde yer alan ve sır teşkil eden bilgiyi hukuka aykırı şekilde elde edip öğrenmeyi,
2) Başkasına zarar vermek için sistemde bulunan bilgileri kullanmayı nakletmeyi ve çoğaltmayı,
3) Başkasına zarar vermek veya kendisine yarar sağlamak maksadıyla sistemi ve unsurlarını tahrip etmeyi, değiştirmeyi, silmeyi ve sistemin işlemesine engel olmayı, yanlış bir şekilde işlemesini sağlamayı,
4) Sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlamayı, dolandırıcılığı,
5) Sistemi kullanarak sahtecilik yapmayı,

bilişim suçları içinde ele almıştır.[4]

Bilişim suçu veya bilgisayar suçu terimi bir bilgisayar ve bilgisayar ağı (Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknoloji) kullanılarak işlenen herhangi bir suçu ifade etmek için kullanılmaktadır. Bilgisayar, bir suçun işlenmesinde kullanılmış olabileceği gibi bir suçun hedefi de olabilmektedir. Bilişim (Siber) suçları bireylere veya birey gruplarına yönelik, mağdurun onurunu zedelemeye veya mağdura fiziksel veya zihinsel olarak doğrudan veya dolaylı olarak zarar verme suçu kastı ile İnternet (görüşme odaları, epostalar, ilan sayfaları ve gruplar) ve cep telefonu (SMS/MMS) gibi çağdaş iletişim araçları kullanarak zarar verme amaçlı saldırıların yapılmasıdır. Bu tür suçlar bir ulusun güvenlik ve ekonomik bütünlüğüne yönelik bir tehdit de oluşturabilmektedir. Bu tür suçlarda ortaya çıkan görünüm, özellikle yazılım CD'lerinin şifrelerinin kırılması, telif hakları ihlalleri, çocuk pornografisi ve çocukların diğer biçimlerde istismarı konularında yüksek kazanç elde etme isteğidir. Mahrem bilgilerin kaybedilmesi veya yasaya aykırı olarak elde edilmesi durumlarında özel yaşamın gizliliğinin ihlali suçu ortaya çıkmaktadır.

Dünya bilişim suçları olgusu ile 1960'lı yılların sonunda tanışmıştır. Kişisel verilerin toplu olarak işleme tabi tutulduğu veri bankalarının oluşmasıyla gizliliğe karşı sorunlar ve tehditler başlamış ve ilk olarak bilgisayar manipülasyonu, sabotaj ve casusluk suçları görülmüştür. 1970'lerde bilişim ağlarının kullanılmaya başlamasıyla hackleme türünden bilgisayar korsanlığı fiilleri, 1980'lerde kişisel bilgisayarın kullanımının yaygınlaşmasıyla program

[4] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

korsanlığı fiilleri artış göstermiştir. Aynı süreçte ATM'lerin bankacılık işlemlerinde kullanılmaya başlanması banka kartları ile ilgili suçları beraberinde getirmiştir[5]

Uluslararası alanda bilişim suçlarıyla ilgili olarak ilk kanun tasarısı Amerika Birleşik Devletleri Kongresine 1977 yılında verilmiştir. Amerika Birleşik Devletleri, bilgisayarın anavatanı olması nedeniyle bilişim suçlarıyla ilk defa karşılaşan ülke olmuştur. Bunun doğal sonucu olarak hem öğreti hem yasal düzenlemeler hem de uygulamada ABD merkez ülke konumundadır.[6]

Uluslararası alanda hem devlet hem de devlet dışı oyuncular istihbarat, malî hırsızlık gibi konularda siber suçlarla ve diğer sınır ötesi suçlarla meşgul olmaktadır. Uluslararası sınırları aşan ve en azından bir ulus devletin çıkarlarını ilgilendiren eylemler siber savaş olarak değerlendirilmektedir. Uluslararası yasal makamlar bu oyuncuların eylemlerinden ötürü uluslararası suç mahkemelerinde hesap vermelerini sağlamaya çalışmaktadır.[7]

Bilgi teknolojilerinin hızla gelişimi, bu gelişmelere aynı hızda ayak uydurabilecek bir toplum yapısı geliştirme ihtiyacını doğurmuştur. Özellikle Bilişim teknolojilerinin gelişmesi sonucunda yaşanan ekonomik ve kültürel ve sosyal alandaki değişmeler, toplumun her alanında değişimi beraberinde getirmektedir. Dijital iletişim alanındaki gelişmeler hayatımızı geri dönülmeyecek bir biçimde değiştirmiştir ve değiştirmeye de devam etmektedir. İnternet dünyası ve bilişim teknolojilerinde yaşanan değişimler, sosyal ilişkilerimizi doğrudan etkilemekte ve sosyal hayatımızı şekillendirmektedir. Fikir ve ifade özgürlüğü internet sayesinde hiç olmadığı kadar gelişmiştir. Bu yeni özgürlük alanı, bir yandan da dev bilgi deposu ve kayıt alanı olarak gelişimini sürdürmektedir. Küreselleşme süreci de bu alanı hem genişletmiş hem de karmaşık hale getirmiştir. "Dünyanın tek bir mekân olarak algılanabilecek ölçüde sıkışıp küçülmesi anlamına gelen bir süreci" ifadesiyle tanımlanan küreselleşme, ekonomik, siyasal, sosyal ve kültürel değerlerin ve bu değerler çerçevesinde oluşmuş birikimlerin ulusal sınırlar dışına taşarak dünya geneline yayılması şeklinde değerlendirilmektedir. Ekonomik açıdan bakıldığında, Bilişim teknolojisindeki gelişmelerle birlikte, sanayi ekonomisi yerini bilgi ekonomisine bırakırken, ekonominin üçlü sacayağı olarak nitelendirdiğimiz üretim, tüketim, dağıtım ilişkileri ve ekonomik yapının tümü, bilgi

[5] ALTUNOK Ebru, VURAL Ali Fatih, Bilişim Suçları, s.2, 2011/8 https://dergipark.org.tr/tr/download/article-file/208853
[6] https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/
[7] https://tr.wikipedia.org/wiki/Bili%C5%9Fim_su%C3%A7lar%C4%B1

temeli üzerine yeniden yapılanmış ve bilgi rekabetin temel faktörü durumuna gelmiştir. Kültürel değişimler açısından bakıldığında, özellikle internet medyasının getirdiği özgür ve geniş alan, sosyal medyanın en büyük paylaşım alanı olmasını sağlamıştır.

Bilişim teknolojilerinin hızlı bir şekilde gelişmesi sonucunda internet faydalarının yanı sıra art niyetli kişilerin ulaşması kolay, izlerinin diğer suçlara göre daha zor bulunacağı, sanal bir suç işleme ortamı sunmuştur. Teknolojiye bağlı olarak bilişim alanına kazandırılan her türlü araca bağlı olarak işlenen suç şekilleri de sürekli gelişmektedir. İnternetin özellikle hukuksal alanda pek çok davranış şekilleri ile birlikte yeni sorunları da beraberinde getirdiği yaşanan bir gerçek haline gelmiştir. Siber suçlar ya da Bilişim suçları yaygın olarak; sahte internet siteleri (phishing, pharming amaçlı) oluşturma, kişilerin şifreleri ve kullanıcı bilgilerini ele geçirme, web sitelerine ve sunucularına yönelik saldırılar düzenleme (defacement-bozma), virüs taşıyan e-postalar (spam mail) yollayarak elektronik saldırılar yapma gibi çeşitli şekillerde gerçekleştirilmektedir. Mağdurun bilgisi ve rızası dışında ele geçirilen şifre, kullanıcı adı, resim, görüntü gibi bilgi ve dokümanlar şahsa karşı; karalama, şantaj gibi suçları işlemek üzere kullanılmaktadır. Bilişim suçlarının kendine özgü niteliği nedeniyle fail kurbanlarından fiziksel olarak uzaktadır. Aynı zamanda işlenen fiilin suç olup olmadığı geleneksel suçlarda olduğu gibi siyah ve beyaz ayrımından ziyade gri alan içerisinde kalmaktadır. Failler bu eylemi gerçekleştirirken kasıtlı hareket etmektedirler ve belirli bir amaçları vardır.[8]

1.1 İnternetin Tarihi Gelişimi ve Temel Kavramlar

Bilgisayarların, çeşitli yöntemlerle birbirine bağlanabilir hale gelerek bilgisayar ağları oluşturmaya başlaması, bilişim teknolojilerinin gelişmesini ve dünyada bilginin küreselleşerek kendisini daha hızlı üretmesini ve dönüştürmesini sağlamıştır. Kuşkusuz ki, teknolojik gelişmeleri tetikleyen en önemli olay, dünya çapındaki küçüklü büyüklü bilgisayar ağlarının kurulması ve varlığı değil, bütün bilgisayar ağlarını kapsayan genel bir ağ olan "internet" in tesis edilmesi olmuştur. İnternet, birden fazla haberleşme ağının (network), birlikte meydana getirdikleri bir iletişim ortamıdır. Bu iletişim ağları, bilgisayarlar ile örülmüştür. Yani, internet bilgisayarlar arasında kurulmuş bir haberleşme ağıdır. İnternet, kişilerin dünya üzerinde birbirleri ile çok geniş amaç ve içerikte iletişim kurmalarını, bilgi alışverişinde bulunmalarını

[8] YILMAZ Furkan, GÜLLÜPINAR Fuat, Türkiye'de Bilişim Suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi, https://dergipark.org.tr/tr/download/article-file/1169453

sağlayan ortak iletişim alt yapısıdır. Ancak, internet dünyadaki bilgi ağlarının tamamı olmayıp, dünya çapında çok sayıda bilgisayara ve bilgisayar ağlarına bağlantı kurabilen ve bunu dünya çapında kabul edilen bilgi ağları protokolüne (TCP/İP) bağlı olarak, özel bir ağ mimarının tanınması vasıtasıyla gerçekleştirerek bilgiye erişim sağlayan bir bilgi ağıdır. Belli bir merkezi olmayan, geniş seviyede planlanmış hiyerarşik bir yapısı bulunmayan küresel bir ağ yapısı olarak da nitelendirilen internet, kişilerin dünya üzerinde birbirleri ile çok geniş amaç ve içerikte iletişim kurmalarını, bilgi alıp vermelerini sağlayan bir ortak haberleşme altyapısı olarak dünya yüzünde gerçekten hızla yaygınlaşmıştır.

İnternet sözcüğünde yer alan "net" ifadesi bilgisayar ağı anlamına gelmektedir. Bu ağların birbirleriyle bağlantı kurmaları ile gelişen bir "Ağ Sistemi" ortaya çıkmaktadır. Bu ağ sistemi aracılığıyla iletişim kuran milyonlarca bilgisayar birbirlerine haber ve bilgi iletmektedir. Bu ağ, ortamda yer alan her türlü bilgiye ulaşım kolaylığı sağladığı gibi, dünyanın farklı yerlerindeki kullanıcıların birbirleriyle iletişim kurmalarına da imkân sağlamıştır. Günümüzde kişilerin birbirleriyle yazılı, sesli ve görüntülü olarak iletişim kurulabildiği kişisel ve kitle iletişim yöntemlerinden en önemli ve yaygın olarak kullanılanlarından birisi internettir. Ama öncelikle internet için söylenmesi gereken husus bir bilişim sistemi olduğudur. Geniş anlamda bilişim sistemi, bilgi ve verileri otomatik olarak işleyen bir sistemdir. Milattan önce sayma işlemine yarayan abaküs ile başlayıp 1800'lü yıllarda hesap makinelerinin geliştirilmesi ile ortaya çıkan bilgisayar 1945'lerde askeri amaçlarla geliştirilmiş; 1970'lerden itibaren ise hafızasının yükselmesi ve işlem hızı ile artık vazgeçilmez bir tekno organ olmuştur. İnternetin tarihçesine baktığımızda askeri amaçlarla Amerika Birleşik Devletleri (ABD) tarafından geliştirildiği görülmektedir. 1957 yılında Sovyetler Birliği'nin Sputnik uydusunu uzaya göndermesinin ardından Amerika, ortaya çıkacak bir savaş veya karışıklık halinde Dünyanın çeşitli yerlerine yerleştirilmiş savaş sistemlerini bir bilgisayar ağı ile yönetme kararı vermiştir. Bu doğrultuda merkeze bağımlılığı olmayan ayrı ayrı çalışabilen bilgisayarlardan oluşan bir ağ kurulabilmesi hedeflenmiştir. Bu amaçla Savunma Bakanlığı'nda ARPA isimli bir birim oluşturulmuş ve bu birim bazı askeri projelerin birbirinden uzakta olan bilgisayarların birbirine bağlanması yoluyla desteklenmesi üzerine çalışmalara başlamıştır. Önce ABD'nin California ve Utah eyaletleri arasında dört ayrı merkez arasında 1969 yılında bilgi transferi gerçekleştirilmiş, sonra bu model geliştirilerek ARPANET isimli askeri bir bilgisayar ağı kurulmuştur. ARPANET'e bağlı bilgisayarlar farklı tipte oldukları için TCP/IP adı verilen bir dil geliştirilerek bu bilgisayarlar arasında iletişim kurmaya başlanmıştır. 1980 yılında TCP/IP protokolü sivil kullanıma da açılmıştır. Bilgisayarlar arasında iletişim sağlayacak bu ortak dilin sivil hayatta kullanıma

açılması sonucu 1980'li yıllarda İngiltere ve Japonya gibi ülkelerdeki bilgisayarlar birbirleriyle iletişime geçebilmişlerdir. 1989 yılında Cenevre'deki bir araştırma merkezinde World Wide Web (www) geliştirilerek internet kullanıcılarının birbirleriyle daha rahat iletişim kurmaları sağlanmış, 1990 yılında ise World Wide Web'in dayandığı en temel dosya protokolü olan Hyper-Text Transfer Protocol (HTTP) geliştirilmiştir. Özel sektör kuruluşlarının 1990'lı yılarda kendi ağlarını geliştirmeleri sonucu internet askeri ve resmî kurumların yönlendirmesinden çıkmış günümüzdeki halini almıştır[9].

1.1.1 Temel Kavramlar

İnternetin daha iyi anlaşılabilmesi için öncelikle bilgisayardan başlayarak en çok kullanılan bazı kavramlar şu şekilde tanımlanmaktadır.

Bilgisayar, kullanıcılardan aldığı verilerle aritmetik ve mantıksal işlemleri yapabilen ve yaptığı işlemlerin sonuçlarını saklayabilen, saklanan bilgilere istenildiğinde ulaşılabilen elektronik bir makinedir. Bir başka şekilde de uzun ve karmaşık hesapları dahi büyük bir hızla yapabilen, lojik (mantıksal) bağlantılara dayalı karar verip, işlem yürüten "makine" olarak tanımlanabilmektedir.

Veri, bilişim sistemlerinin en temel birimidir. Bilişim sistemlerinin amacı, veriyi saklamak, işlemek ve sonuç çıkarmaktır. Veri, bilgilerin belirli bir formata dönüştürülmüş halidir. Veri; her türlü bilginin, bilgisayarın işlem yapabileceği, sonuçlar üretebileceği, saklayabileceği ve gerektiğinde yeniden okuyabileceği şekilde sayısal birimlere dönüştürülmüş halidir.

Bilgisayar programı, bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak düzene konulmuş komut dizilimidir. Bilgisayarın çalışmasının temelinde işletim sistemi adı verilen ve bilgisayarın çalışabilmesi için gerekli veriler, komutlar ve dosyaları içeren ana program vardır. Bilgisayar açıldığı zaman harekete geçen ve otomatik olarak yüklenen dosyalar ve komutlar, kullanıcının bilgisayarda işlem yapabilmesini sağlayan zemini oluşturmaktadır. Dos, Windows, Linux, Zenix gibi farklı işletim sistemleri mevcuttur. İşletim sistemi de temelde bir bilgisayar programıdır ve bilgisayarın hangi durumda nasıl davranması gerektiğini bildiren komutlar içermektedir.

[9] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

Arayüz (İnterface), farklı iki yazılım, iki donanım ya da yazılım-donanım arasındaki uyumu sağlamak, istenmeyen etkileri önlemek amacıyla kullanılan ortak sınır olarak tanımlanabilmektedir. Daha genel anlamda, bir mekanizma ile onun kullanıcısı arasındaki etkileşime aracılık eden yüzeye veya ortama denmektedir. Bilgisayar teknolojisinde kullanılan arayüzler ikiye ayrılmaktadır:

- **Komut Satırı Arayüzü:** Kullanıcının yazarak girdiği komutlarla iş görmektedir (Örnek, DOS).
- **Grafiksel Kullanıcı Arayüzü:** Fare, oyun çubuğu gibi yan araçlar yardımı ile iş görmektedir (Örnek: Windows, KDE, Gnome).

TCP/IP Protokolü, "Bilgi ağı" üzerindeki bilgi iletimi ve paylaşımı bazı kurallar dâhilinde yapılmaktadır. Bu kurallara, internet protokolleri ya da TCP/IP (Transmission Control Protocol/ Internet Protocol) protokoller ailesi denmektedir. Bu protokoller birbirleriyle iletişim kuran milyonlarca bilgisayardan oluşan bir ağda yer alan farklı yapıdaki bilgisayarların birbirleriyle iletişim kurabilmeleri için oluşturulan bir anlaşma dilidir. Transport Control Protokol sözcüklerinin kısaltılmış hali olan "TCP" iletim kontrol protokolü anlamına gelir ve mesajların doğru yere ulaştırılmasından; "IP" ise internet protokolü anlamına gelir ve adresleme sisteminden sorumludur.

İnternet hizmetlerini kullanabilmek için gerekli olan tüm yazılımlar ve bağlantı yazılımları, TCP/IP protokolüne uygun olarak iletişim kurmakta ve işlev görmektedirler. Bu protokollere örnek olarak, internet üzerindeki bilgisayarlar arasında dosya alma/gönderme protokolü FTP (File Transfer Protocol), Elektronik posta iletişim protokolü (SMTP Simple Mail Transfer Protocol), internet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen "login" protokolü (TELNET) verilebilmektedir. Adını sıkça duyduğumuz www (ya da web) ortamında birbirine bağlanmış farklı türden objelerin iletilmesini sağlayan protokol ise Hyper-Text Transfer Protocol (HTTP) olarak adlandırılmaktadır.

World Wide Web (www) kısaca web; birçok internet hizmetini birleştiren bir araç olarak; yazı, resim, ses, video, animasyon gibi pek çok farklı nitelikteki verilere etkileşimli olarak ulaşmamızı sağlayan çoklu hiper ortam sistemidir. Bütün bu farklı yapılardaki veriler uygun bir standart ile bir arada kullanılarak bir web tarayıcısında görüntülenebilmektedir. Hiper ortam, bir dokümandan başka bir dokümanın çağrılmasına (navigate) imkân vermektedir (iç içe dokümanlar). Bu ortamdaki her veri (object), başka bir veriyi çağırabilmektedir (link). Link,

aynı doküman içinde başka bir yer olabildiği gibi, fiziksel olarak başka bir yerde de (internet üzerindeki herhangi bir makinada) olabilmektedir. Bütün bu farklı yapıdaki veriler uygun bir standart ile bir arada kullanılıp bir web tarayıcısında (web browser) görüntülenebilmektedir. Web'in diğer bir işlevi de öteki bazı internet servislerini kendi içerisinde barındırmasıdır (ftp, gopher, news, wais vb.). Web uygulamaları (Web sayfaları), web listeleyicilerinde /tarayıcılarında (Browser, Gezgin, Tarayıcı) görüntülenebilmektedir. Web sayfaları, başka sayfalara ve değişik türden verilere hiper linkler içermektedir. Buralara fare (mouse) ile tıklayarak, başka sayfalara, oradan da başka sayfalara geçmek mümkündür. Bu aslında çok basit olarak bir bilgiye ulaşım modelidir.

Web Sistemleri, kullanılan platformdan bağımsızdır. Bir Macintosh, PC ya da Unix Web listeleyicisi aynı sayfaları, aynı şekilde almaktadır. Sayfaların alındığı web servisleri de farklı bilgisayar platformlarında olabilmektedir. Web listeleyicileri ve web servis sağlayıcı ortamlar hemen hemen tüm dünyada her yerde vardır ve global olarak kullanımları üstel bir şekilde artmaktadır. Web yapısının bu kadar çok kabul görmesinin sebepleri, web'in açık bir sistem olması, Platform, bilgisayar, işletim sistemi vb. ile bağımlı olmaması ve web üzerinden pek çok bilgi kaynağına kolayca erişilebilmesidir. Web uygulamaları geliştirmek ve bunları kullanıma sunmak çok kolaydır[10].

Web Browser (web tarayıcısı), internet üzerindeki tüm bilgilere bakabilme ve bu bilgilerle etkileşim halinde olabilme imkânı veren bir uygulama programıdır. Web tarayıcısı ile web adreslerine erişilebilmektedir. Bilgisayar kullanıcısının internet aracılığıyla bir web hizmet merkezine bağlandıktan sonra tek seferde ekranına aktarabildiği yazı resim grafik veya ses bilgilerini içeren farklı verilerden de oluşabilen web sayfası, HTML (Hyper-Text Markup Language) adı verilen işaretleme dili kullanılarak oluşturulmaktadır. Bu işaretleme dili sayesinde bir web sayfasında hangi kelime veya cümleye tıklandığında hangi sayfaya bağlanılacağı web sayfasındaki resimlerin nereden alınacağı ve sayfaya ilişkin unsurlar işlev kazanmaktadır.

[10] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

Microsoft İnternet Explorer, diğer adıyla ağ tarayıcısı, kullanıcıların ağ sunucuları üzerinde yer alan HTML sayfalarını açmasını sağlayan yazılımdır. En yaygın kullanılan tarayıcılar, Microsoft İnternet Explorer, Mozilla, Firefox ve Safari'dir[11].

Domain Name (DNS, Domain Name System/alan adı sistemi), olarak adlandırılan hiyerarşik bir isimlendirme sistemi ile (alan adı sistemi), internete bağlı bilgisayarlara ve bilgisayar sistemlerine isimler verilmektedir. DNS de aslında bir TCP/IP servis protokolüdür. DNS, 'host' olarak adlandırılan internete bağlı tüm birimlerin yerel olarak bir ağaç yapısı içinde gruplandırılmasını sağlamaktadır. Bu şekilde, bütün adreslerin her yerde tanımlı olmasına gerek kalmamaktadır. Her bir internet adresine 4 haneli bir numara karşılık gelir. a.b.c.d şeklindeki bu numaralara IP (İnternet Protocol) numaraları denilmektedir. Burada, a.b.c ve d 0-255 arasında değişen bir tam sayıdır. (32 bit adresleme sistemi).

Her internet adresinin ilk kısmı bulunduğu domain'in network adresini, son kısmı ise makinenin (host) numarasını verecek şekilde ikiye bölünmüştür. İnternet üzerindeki her bilgisayarın o anda sadece kendisine ait olan bir adresi vardır. Statik IP sürekli size ait olan bir IP adresinin olması ve bilgisayarınıza tanımlanmasıdır.

İnternet ağını oluşturan her birim sadece kendine ait bir IP adresine sahiptir. Bu IP adresleri kullanıcıların kullanımı için www.site_adı.com gibi kolay hatırlanır adreslere karşılık düşürülmektedir. DNS sunucuları, internet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır. Sistem makine isimlerini IP adreslerine, IP adreslerini ise makine isimlerine çevirmektedir. Bir DNS istemci bir bilgisayarın ismine karşılık IP adresini bulmak istediği zaman isim sunucuya başvurmaktadır. İsim sunucu, yani DNS sunucu da eğer kendi veri tabanında öyle bir ad varsa, bu ada karşılık gelen IP adresini istemciye göndermektedir. DNS veri tabanına kayıtların elle, tek tek girilmesi gerekmektedir. DNS üstlendiği görev gereği hızlı olmak zorundadır.

İnternet adresleri ilk önce ülkelere göre ayrılmaktadır. Adreslerin sonundaki tr, de, uk gibi ifadeler adresin bulunduğu ülkeyi göstermektedir. Örneğin tr Türkiye'yi, de Almanya'yı, uk İngiltere'yi göstermektedir. DNS ve benzeri uygulamaları yaratan ülke ABD olduğundan ABD adresleri için bir ülke takısı kullanılmamaktadır. ABD'ye özel kuruluşlar için us uzantısı yaratılmıştır. İnternet adresleri ülkelere ayrıldıktan sonra com, edu, gov gibi daha alt bölümlere

[11] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

ayrılmaktadır. Bu ifadeler DNS'de üst düzey (top-level) alan adlarına karşılık gelmektedir. Üst düzey alan adlarında; com: Ticari kuruluşları, edu: Eğitim kurumlarını, org: Ticari olmayan, hükümete de bağlı bulunmayan kurumları, net: İnternet omurgası işlevini üstlenen ağları, gov: Hükümete bağlı kurumları, mil: Askeri kurumları, num: Telefon numaralarını bulabileceğiniz yerleri, arpa: Ters DNS sorgulaması yapılabilecek yerleri göstermektedir. Bu isimlere biz veya tv gibi isimler de eklenmiştir.

Alan adları, ağaç yapısı denilen ve belli bir kurala göre dallanan bir yapıda kullanılmaktadır. Amerika haricinde, internete bağlı olan tüm ülkelerdeki adresler, o ülkenin ISO3166 ülke kodu ile bitmektedir. Türkiye'deki tüm alt alan adresleri, .tr ile bitmektedir. Örneğin; marine.ulakbim.gov.tr adresinde: tr Türkiye'yi, gov alt alanın devlet kurumu olduğunu, ulakbim bu devlet kurumunu, marine bu kurumda bulunan bir makinayı göstermektedir.

Elektronik Posta (E-Mail, E-Posta), internete bağlı çok sayıdaki kullanıcının birbirleriyle haberleşebilmek için kullandıkları elektronik mesaj iletim sistemidir. İnternet hizmetleri içinde en çok kullanılan hizmet türü e-mail'dir. E-mail geleneksel posta sistemi ile aynı işleve sahip olan bir iletişim türüdür. 1971 yılında geliştirilen e-mail başlangıçta sadece düz yazı mesajlar göndermek amacıyla kullanılabilirken, 1995'ten itibaren teknolojik ilerleme ile e-maille resim, ses, video, html dokümanları, çalışabilir program vb. iletme mümkün hale gelmiştir. E-mail sisteminden yararlanabilmek için kullanıcıların bir e-mail adresine sahip olmaları gereklidir. E-mail adresleri, kullanıcılara erişim sağladıkları servis sağlayıcı aracılığıyla sağlanabileceği gibi, internet üzerinde bulunan çok sayıdaki e-mail sistemlerinden de ücretsiz olarak temin edilebilmektedir. Bir e-mail adresine sahip olan herkes, bir internet bağlantısını kullanarak e-mailin sağladığı imkânlardan yararlanabilmektedir. Alıcıya gönderilen e-mail mesajları bilgisayarın belleğine veya CD/diskete kaydedilebileceği gibi bir yazıcı yardımıyla basılabilmektedir veya başka kullanıcılara yine e-mail yoluyla gönderilebilmektedir. Gönderilen e-mail mesajları, alıcı için ayrılan dijital e-mail kutusunda depolanmakta ve alıcı dilediği an herhangi bir yerde bulunan internet bağlantısını kullanarak e-mail kutusunu açarak mesajlarına ulaşabilmektedir.

Elektronik postaların çok güvenli olduğu söylenememektedir. E-mail bir yere ulaşırken pek çok domain'den geçebilmekte ve buralarda istenilirse e-maillerin içeriğine bakılabilmektedir. İnternetteki güvenlik sorunları, ticari kullanımın artmaya başladığı 1995'ten itibaren ciddi olarak ele alınmıştır. Birçok e-mail adresinin ana server'ı, hosting'i Amerika Birleşik

Devletleri'nde yer almaktadır. Dünyanın internet alt yapısına sahip olan ülkesi de ABD olduğundan istenir ise bütün e-mailler ABD tarafından okunabilmektedir. Okunmasa da e-maillerin bir kopyası saklanmaktadır.

Telnet, internet ağı üzerindeki bir makineye uzaktan bağlanmak için geliştirilen bir TCP/IP protokolü ile bu işi yapan programlara verilen genel isimdir. Telnet sistemi, bilgiye daha kolay ve hızlı ulaşabilme gereksiniminin bir sonucudur. Bu nedenle, bu sistemi en çok kullanan kuruluşlar kütüphanelerdir. Örneğin, İstanbul'dan veya ülkenin herhangi bir yerinden ODTÜ Kütüphanesi'ne ve ABD Kongre Kütüphanesi'ne telnet sistemi ile ulaşılabilmektedir.

Aktarma Protokolü (FTP), internete bağlı bilgisayarlardan birinden diğerine iki yönlü olarak dosya aktarımı yapılabilmesini sağlayan protokoldür. FTP ile iki şey yapılmaktadır; birincisi büyük dosyaların herhangi bir sorunla karşılaşmadan uzak mesafelere aktarılması, ikincisi ise aktarılan dosyanın doğrudan bilgisayarın belleğinde bir dosyaya yerleştirilerek orada saklanmasıdır. FTP'lerde genellikle ücretsiz olarak erişilebilen çok değişik türden malzeme bulunmaktadır. Bunlar yazılı metinlerle birlikte grafikler, sesli yapıtlardan oluşabilmektedir. İnternet üzerinden dosya aktarımı dosya bütünlüğünün korunamaması, bilgisayar güvenliğinin sağlanamaması ve telif hakkı sorunları gibi durumları içeren pek çok sorunu beraberinde getirmektedir[12].

Bilişim, Sözlük anlamıyla "insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi" olarak tanımlanmakta ve Fransızca kökenli "enformatik", "informatik" terimlerine karşılık gelmektedir. Almanca 'da "informatik", İngilizce 'de "informatic" ve İtalyanca 'da "informatica" olarak kullanılmaktadır. Bilişim hem verilerin işlenmesini, yani bilgi işlemi, hem de bilgi işlemin sonucunun aktarılmasını, yani veri iletişimini ifade eden bir kavramdır. Teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır.

Açık Anahtar Altyapısı (AAA): Bir mesajı gönderenin ya da alanın kimliğini doğrulamak ve/veya bir mesajı şifrelemek için kullanılan bir yöntemdir. AAA, internet gibi güvenli olmayan

[12] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

kamusal bir ağın kullanıcılarının, güvenilir bir yetkiliden alınan ve onun aracılığıyla paylaşılan bir kriptografik anahtar çifti kullanarak güvenli ve gizli bir şekilde veri değişimi yapmalarını sağlamaktadır. Bir kişi ya da kuruluşun kimliğini tanımlayan sayısal sertifikaların ve sertifikaları saklayabilen, doğrulayabilen ve gerektiğinde iptal edebilen dizin hizmetlerinin kullanımına imkân vermektedir.

Günümüzde internet kullanımının yaygınlaşması özellikle elektronik bankacılık ve elektronik ticaret sistemleri ile elektronik haberleşme ve elektronik eğitim platformlarının kullanımını beraberinde getirmiştir. İnsanların evden veya işyerlerinden tüm ihtiyaçlarını elektronik platform ve uygulamalar ile yürütmesi kullanım açısından çok büyük kolaylıklar sağlamakla birlikte; özellikle elektronik bankacılık ve elektronik ticaret platformlarındaki güvenlik açıkları neticesinde ortaya çıkan kayıplar (ticari casusluk, para aktarımı, yetkisiz erişim vs.) çok büyüktür. Özellikle bu uygulamalarda kullanılan statik şifreler ile buna benzer statik kimlik tanıma yöntemleri güvenliğin sağlanmasında aktif rol oynasa da gerçek bir kimlik tanıma işlevi sağlamamaktadırlar. Dolayısıyla, başta bankacılık işlemleri olmak üzere pek çok sektörde tam ve güvenli olarak elektronik ortamda işlem yapılabilmesi için, onay ve yetki güvenliğinin sağlanması, giderilmesi gereken eksikliklerin başında yer almaktadır. Keza, internet üzerinde yapılan işlemlerde, elektronik mesaj gönderen veya işlem gerçekleştiren kişinin kimliğinin belirlenmesinin, yasalar önünde delil niteliği taşıması ihtiyacı nedeniyle dijital sertifika sistemi oluşturulmuştur. Tüm dijital sertifika sistemleri PKİ (Public Key İnfrastructure) Açık Anahtar Altyapısı üzerine kurulmuştur.[13]

Bilgi Toplumu: Bilgi ağları ve Bilgi İletişim Teknolojileri (BİT)'ni yaygın bir şekilde kullanan, büyük miktarlarda bilgi ve iletişim ürünleri ve hizmetleri üreten, çeşitlendirilmiş içerik endüstrisine sahip bir toplumdur.

Bilgi Ağı: Kullanıcılara verilen bir bilgi kümesi için erişim ve üretim hizmetleri sunan BİT, donanım ve hizmetler sistemine (örneğin elektronik posta, dizinler ve video hizmetleri) verilen addır. Bilgi ağı altyapısı ise, iletim bağlantıları, erişim prosedürleri, hukuki ve genel çerçeve ile bilgi ağının temel ve destekleyici hizmetlerini içeren sistemin tümünü anlatmaktadır.

[13]Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

Bilgi Teknolojileri (BT): Verilerin elektronik ortamda işlenmesi ve aktarımı için kullanılan donanım, yazılım ve yöntemlerini ifade etmektedir.

Bilgi ve İletişim Teknolojileri (BİT): Çeşitli biçimlerdeki bilgiyi oluşturmak, saklamak, düzenlemek, yönetmek, taşımak, görüntülemek, aktarmak, değiştirmek, iletmek ya da almak için kullanılan bütün teknolojileri içeren her türlü donanım ya da bağlantılı sistem (veya alt sistem) anlamındadır. BİT hem bilgisayar hem de iletişim teknolojilerini ifade etmektedir.

Bilgi Yönetimi (BY/İnformation Management): Bir bilgi işlem sisteminde bilginin elde edilmesi, incelenmesi, muhafaza edilmesi, geri getirilmesi ve dağıtılmasını kontrol eden fonksiyonlardır[14].

Bilişim Sistemi, Yeni Türk Ceza Kanunu'nun 243. madde gerekçesinde, Bilişim sistemi, "veri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir" şeklinde tanımlanırken, Avrupa Konseyi SİBER Suç Sözleşmesi'nin "Tanımlar" başlıklı 1. maddesinde "bilgisayar sistemi" terimi, 'bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihazı ifade edecektir' şeklinde ifade edilmektedir. Bilişim sisteminin biri maddi diğeri de soyut olmak üzere iki bileşeni bulunmaktadır. Bilişim sisteminin, verileri depolamaya, işlemeye, kullanmaya ve nakletmeye yarayan cihazlarına donanım, bunların bu şekilde çalışmasını sağlayan programlara da yazılım denmektedir. Bilişim sistemi, yazıcı, modem gibi tüm çevre birimleri de dâhil olmak üzere bilgisayardan beklenen tüm amaçları gerçekleştirmeye elverişli donanım ve yazılım öğelerinin bütünüdür.

Çevrimiçi Devlet Hizmetleri: Kamu kurumları tarafından bilgi ağları aracılığıyla vatandaşlara, işletmelere ve kuruluşlara (diğer kamu kurumları dâhil) sunulan hizmetlerdir (bu hizmetlerin sağlayıcısının her zaman kamu kurumları olması gerekmemektedir).

E-Devlet: Vatandaşlara devlet tarafından verilen hizmetlerin elektronik en kolay ve en etkin bir biçimde, kaliteli, hızlı, kesintisiz ve güvenli ulaştırılmasını sağlayan yapıdır. Bürokratik ve klasik devlet kavramının yerini alan e-devlet anlayışı ile, her kurum ve bireyin bilgi teknolojilerini kullanan sistemler ile devlete ulaşması hedeflenmektedir.

[14] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

Portal: Çeşitli sağlayıcılardan bilgi ve hizmetleri koordine ederek, kullanıcıların ihtiyaçları doğrultusunda şekillenmiş bir içerikle sunan internet sitesine verilen addır.

Kimlik doğrulama: Kullanıcıların çevrimiçi bir bilgi sistemi ya da uygulamaya erişimine izin vermeden önce kimliklerini kontrol eden bir güvenlik önlemidir.

Kurumsal mimari: Bir kurumun temel amaç ve stratejilerinin kurumun organizasyon süreçleri, bilgi sistemleri, personeli ve birimleri ile uyumu da kapsayan genel yapısıdır.

Zararlı içerik, internet üzerindeki içeriklerin yaklaşık %8'i istenmeyen, zararlı içerik olarak kabul edilmektedir. İstenmeyen içerik 3 başlık altında incelenebilir. Bunlar Yetişkin (Adult), Suç (Criminal) ve Sosyal Sapma (Social Deviance) içerikleridir. Yetişkin (Adult): a) Pornografi, b) Erotik/Seks, Suç (Criminal): a) Anonim proxy'ler, b) Bilişim suçları, c) Yasadışı aktiviteler, d) Sağlık için tehlikeli madde temini, e) Zararlı Yazılımlar, f) Şiddet g) Yazılım hırsızlığı/Yasadışı yazılım/Hacking, Sosyal Sapma (Social Deviance): a) Aşırı Uç/ Irkçılık, b) Sapık inançlar. Zararlı içeriğe karşı Dünyada internetin filtrelenmesi konusunda çeşitli uygulamalar bulunmaktadır. Bazı ülkeler çeşitli gerekçelerle ve herhangi bir hukuki değerlendirmeye ihtiyaç duymaksızın bütün ülke internet trafik çıkışı üzerinden kapsamlı ve sansür anlamında internet filtrelemesi yapmaktadır. AB ülkeleri ise genelde daha çok belirli suçlar çerçevesinde engelleme ve nesne temelli filtreleme işlemi gerçekleştirmekte ya da internet konusunda özel bir kanunla düzenleme yapmak yerine internet ortamında işlenen suçlarla mücadele etmeye çalışmaktadır. Nesne temelli filtreleme birçok ülke açısından ekonomik bulunmamakla birlikte, zararlı içerikten ötürü adeta bir kitap nedeniyle bir kütüphaneyi kapatmaya benzeyen tüm site içeriğine erişimi yasaklama anlayışına tercih edilmektedir. İçlerinde Türkiye'nin de bulunduğu bazı ülkeler ise bu tür içeriklerle ilgili "uyar kaldır (notice an takedown)" yöntemiyle suç unsuru taşıyan kısmi içeriklerin kaldırılması için ilgili internet siteleriyle irtibata geçilmekte, böylelikle sakıncalı içeriklerin kaldırılmasını sağlamayı tercih etmektedir[15].

1.2 Siber Suç Kavramı

Günümüzde bilginin saklanması ve paylaşılması açısından büyük kolaylıklar sağlayan bilişim teknolojileri, bazen kurumlar ve şirketler için önemli maddi ve itibar kaybına neden olabilecek

[15] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

siber güvenlik risklerini ve tehditlerini de beraberinde getirmektedir. Maliyetlerine bakmaksızın en üst düzey güvenlik teknolojilerinden faydalanarak sistemler geliştirilse de bu tür teknik güvenlik önlemleri yeterli olmamaktadır. Çünkü güvenlik teknolojilerinin geliştirilmesi, saldırganları teknik açıdan zorlaşan yapıdaki insan faktörünün zayıflıklarından yararlanmaya yöneltmiştir. Bu durum ise insan faktörünü güvenlik anlamında en zayıf halka haline getirmektedir.

Dünyada bilgisayar ağları üzerinde işlenen suçlara **"Siber Suçlar"** (cyber crimes) tabiri kullanılmaktadır. Siber suç deyimi, bilgisayarlar aleyhine veya bilgisayarlar aracılığıyla işlenen suçlar olarak da tanımlanmaktadır. Herhangi bir suçun elektronik ortam içerisinde işlenebilme imkânı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil, genel olarak hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçları siber suçlar olarak değerlendirilebilmektedir. Siber suç, bilgisayar veya ağ sistemleri yolu ile bilgisayar veya ağ sistemleri içerisinde ya da bilgisayar ve ağ sistemlerine karşı işlenebilmektedir. Siber suçlar daha önceleri kanunlar tarafından Avrupa Konseyi Siber Suç Sözleşmesinin orijinal başlığında yer alan "cyber" kelimesi Türkçe'ye "Siber" olarak çevrilmiştir. Bunun en önemli nedeni Siber sözcüğünün gelişimi içerisinde yüklenmiş olduğu kültürel ve dönemsel anlam bütünlüğüdür. SİBER; Yunanca başdümenci anlamına gelen kybernetes'ten türetilmiştir[16].

Suç olarak tanımlanmış fiillerin Siber ortamda işlenmesi ve daha önce suç olarak tanımlanmamış bu ortamın karakteristiğine has bir takım ihlallerin bir bütünüdür. Siber suç kavramıyla Bilişim suçları ifade edilmekle birlikte, bilişim suçlarının tek bir bilişim sisteminde işlenen şekli değil, bilişim sistem ağları vasıtasıyla (özellikle internet) işlenen suçlar kastedilmektedir. Siber suç "bilgisayarın amaç veya araç veya her ikisi olarak kullanıldığı hukuka aykırı eylem" şeklinde ifade edilmiştir. Birleşmiş Milletler 10. Kongresi'nde siber suçlar, bilgisayar ağlarında veya ağlarına karşı gerçekleştirilen her türlü eylem olarak kabul görmekte ve bu suçlar dar anlamda siber suçlar ve geniş anlamda siber suçlar olmak üzere iki alt kategori içinde değerlendirilmektedir. Bu neviden suçları klasik suç tiplerinden ayıran ve kendine özgü suçlar olmasını sağlayan en önemli özellik, işlenme şekilleridir. Klasik suç tiplerinde suçun maddi unsurunu oluşturan eylemler faillerin fiziki hareketleriyle meydana gelmektedir. Bilişim suçlarında (Siber suç veya internet ortamında işlenen suçlar) ise, genellikle failin bilgisayarın klavyesine dokunması veya mouse tıklaması dışında fiziki hareket

[16] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

olmamakta ancak fiziki hareketlerle meydana getirilebilecek zararlardan çok daha fazlası bu şekilde oluşabilmektedir. Bilişim alanındaki suçlar, bilinen, klasik usullerin dışında çok daha hızlı, kolay ve dikkatlerden uzak işlenebilmekte, tespit edilebilmesi ise daha zor olmaktadır. Bu tür suçlar, sadece çıkar amaçlı yapılmamakta; kimi zaman da toplumda aradığını bulamayan insanların, kendilerini ispat için başvurdukları bir yol olabilmektedir.[17]

1.3 Siber Suçların Sınıflandırılması

Siber suçların hayatımızda yer almaya başlaması ve insanları rahatsız etmesiyle birlikte, bu suçların çeşitli yönleriyle düzenlenmesi ve sınıflandırılması gereği ortaya çıkmıştır. Ceza Hukukunun temel ilkelerinden biri olan "kanunsuz suç ve ceza olmaz" ilkesi uyarınca, kanun koyucuların bu suçlar için düzenlemeler yapması gerektiği ifade edilmiştir. Ancak bu konuda bilgisayar ağları alanındaki sorunların ve özellikle internetin tam olarak değerlendirilememesi, internetin sürekli gelişmesi ve her geçen gün biraz daha fazla insan hayatına girmesi, bunun sonucunda yeni ihlal tiplerinin ortaya çıkması sonucu, cezalandırılması düşünülecek fiillerin hangileri olduğunu saptamaya imkân vermemektedir. Bu nedenle siber suçları sınıflandırma çalışmaları farklılık arz etmektedir.

Siber suçların tarifini yaparken de gördüğümüz gibi herkesin uzlaşmış olduğu bir tanım bulunmamaktadır. Konu ile ilgilenen kimi uzmanlar bu kapsama girmesi muhtemel fiilleri saymakla yetinmekte ve gruplara ayırarak tasnife gerek görmemekte, bazı uzmanlar ise, bu suçları iki, üç ya da dört ana başlık altında incelemektedir.

1.3.1 Birleşmiş Milletler Sınıflandırması

Dünyadaki en büyük örgütlerden birisi olan Birleşmiş Milletler (BM), yaptığı anlaşmalarla üye ülkelerini bağlayıcı kararlar alma gücüne sahiptir. Siber alandaki tehditlere karşı ilk olarak, 1990 yılında gerçekleştirdiği 8. Suçların Önlenmesi ve Suçlulara Muamele Kongresi'nde hazırlanan raporla, BM Genel Kurulunca siber alanı düzenleme konusuyla ilgili kararlara yer verilmiştir (Eight United., 1990). İlerleyen yıllarda ceza ve usul hukukuna bilgisayar ile işlenen suçların engellenmesi ve bu konuda işbirliği yapılmasına dair BM Bilgisayar Bağlantılı Suçların Önlenmesi ve Kontrol Altına Alınması Rehberi eklenmiştir. BM Genel Kurul'u 2001

[17] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

senesinde yine uluslararası alanda işbirliğini sağlamak ve bu teşvik etmek, siber suçlarla mücadele de yetkililere eğitim vermek gibi amaçlarla "Bilgi Teknolojilerinin Kötüye Kullanılması ile Mücadele" adlı kararı almıştır (UN GAOR, 2001). 2005 yılında BM siber alana yönelik siber suçlarla mücadele kapsamında sözleşme için tartışmalara başvursa da örgüt bu kapsamda sözleşme yapmak yerine ülkelere destek vermenin daha verimli olacağını düşünmüştür. Devletlerin çıkarlarındaki farklılıkları ve farklı yaklaşımları, bu alanda gerçekleşecek işbirliğine engel olmuştur.[18]

Bu sınıflandırma yapılırken, İnterpol Genel Sekreterliği'nin hazırlamış olduğu İnterpol Bilgisayar Suçları El Kitabı (Interpol Computer Crime Manual) esas alınmak üzere, Birleşmiş Milletlerin hazırladığı "Birleşmiş Milletler Bilgisayar Suçlarını Kontrol ve Önleme (United Nations on the Prevention and Control of Computer-Related Crime) kitapçığı ve Avustralya Polis Teşkilatı'nın hazırladığı "Bilgisayar Kaynaklı Suçların Soruşturulması için Asgari Şartlar" (Minimum Provisions for the Investigation of Computer Based Offences) kitapçıklarından istifade edilmiştir. Söz konusu sınıflandırmaya göre siber suçlar şunlardır.

1.3.1.1 Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim

Yetkisiz Erişim: Bir bilgisayar sistemine ya da bilgisayar ağına, bir kişinin yetkisi olmadan erişmesidir. Erişim, sistemin bir kısmına ya da bütününe veya programlara veya içerdiği verilere ulaşma anlamandadır. İletişim metodu önemli değildir. Yetkisiz erişim, bir kişi tarafından bir bilgisayara doğrudan yakın bir yerden olabileceği gibi, uzak bir mesafeden örneğin bir modem hattı ya da başka bir bilgisayar sisteminden de olabilmektedir.

Yetkisiz Dinleme: Bir bilgisayar veya ağ sistemi kullanılarak, iletişimin yetkisiz olarak sistem içinden yapılan teknik anlamda dinlemedir. Suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferinin teknik olarak takip edilmesi ve dinlenmesidir. Teknik anlamda dinleme, iletişim içeriğinin izlenmesi, verilerin kapsamının ya doğrudan (bilgisayar sistemini kullanma ya da erişme yoluyla) ya da dolaylı olarak (elektronik dinleme cihazlarının kullanılması yoluyla elde edilmesi ile ilgilidir.

[18] KARADAĞ Şerife, Siber Uzayda Uluslararası Hukuk Mümkün mü?, Selçuk Üniversitesi, 2019 http://sssjournal.com/Makaleler/1545056113_06_5-36.ID1522_Karada%c4%9f_2827-2833.pdf

Suçun oluşması için hareketin yetkisiz ve kasten işlenmesi gerekir. Uygun yasal şartlar çerçevesinde, soruşturma yetkililerinin yaptıkları dinleme bu kategoriye girmez.

Hesap İhlali: Herhangi bir ödeme yapmaktan kaçınmak niyetiyle bir başkasının bilgisayar sistemlerinden erişilebilen hesabını kanunsuz olarak kullanılmaktır. Başka bir ifadeyle bir kişinin, internet, telefon veya benzer bir sistemdeki hesabının kişinin rızası olmaksızın, kanunsuz olarak kullanılmasıdır[19].

1.3.1.2 Bilgisayar Sabotajı

Mantıksal Bilgisayar Sabotajı: Bir bilgisayar ya da iletişim sisteminin fonksiyonlarını engelleme amacıyla bilgisayar verileri veya programlarının sisteme girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir. O halde mantıksal bilgisayar sabotajı, bir bilgisayar ya da iletişim sisteminin fonksiyonlarına zarar vermek amacı ile verilerin veya programların "zaman bombası", "Truva atları", "virüsler", "solucanlar" gibi yazılımlar kullanılarak değiştirilmesi, silinmesi, ele geçirilmesi ya da çalışmaz hale getirilmesidir.

Fiziksel Bilgisayar Sabotajı: Bir bilgisayara ya da iletişim sistemini oluşturan parçalara, sistemin fonksiyonlarını yerine getirememesi amacıyla fiziksel yollarla zarar verilmesidir.

Bilgisayar Yoluyla Dolandırıcılık: Bilgisayar ve iletişim teknolojileri kullanılarak verilerin alınması, değiştirilmesi ve silinmesi yoluyla kendisine veya başkasına yasadışı ekonomik menfaat temin etmek için mağdura zarar vermektir.

Suçlunun hedefi kendisine veya bir başkasına mali kazanç sağlamak ya da mağdura ciddi kayıplar vermektir. Bilgisayar dolandırıcılığı suçları, suçların modern bilgisayar teknolojileri ve ağ sitemlerinin avantajlarını değerlendirmeleri yoluyla klasik dolandırıcılık suçlarından farklılık göstermektedir.

Banka Kartı Dolandırıcılığı: Kartlı ödeme sistemleri kullanılarak yapılan dolandırıcılık ve hırsızlık suçlarıdır. Kredi kartları, bankamatik kartları ve benzeri kartlarla yapılan dolandırıcılık suçlarıdır. Kart ödeme sistemleri (ATM-Automated Teller Machine) genelde bankalar veya

[19] TURHAN Oğuz, Siber Suçlar, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf

benzer finans kuruluşlar tarafından kullanılmaktadırlar. Erişim genellikle bir kişini tanımlama numarası (PIN-Personal Identification Number) girişi gerektiren, bir kart ya da benzeri bir sistem ile yapılmaktadır. Dolandırıcılık bu kartların çalınması, çoğaltılması, kopyalanması veya iletişim hatlarının engellenmesi ve dinlenmesi yoluyla oluşmaktadır.

Girdi/Çıktı/Program Hileleri: Bilgisayar sistemine kasıtlı olarak yanlış veri girişi yapmak veya sistemden yanlış çıktı almak ya da sistemdeki programların değiştirilmesi yoluyla yapılan dolandırıcılık ve hırsızlıktır. Bir bilgisayar veri tabanına yanlış veri girmek, yaygın bir dolandırıcılık yoludur. Davalar araştırılırken sistemde kullanılan yazılım programlarını da içerecek şekilde tam bir teknik tanımlama yapılmasına ihtiyaç vardır.

İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma: Kendisine veya başkasına ekonomik menfaat sağlamak maksadıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerini veya diğer bilgisayar sistemlerini hakkı olmadan kullanmaktır.

Bilgisayar Yoluyla Sahtecilik: Kendisine ve başkasına yasadışı ekonomik menfaat temin etmek ve mağdura zarar vermek maksadıyla, bilgisayar sistemlerini kullanarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturmak veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmaktır.

Bilgisayar Yazılımının İzinsiz Kullanımı: Kanunla korunmuş yazılımların izinsiz olarak çoğaltılmasını, yasadışı yöntemlerle elde edilen bilgisayar yazımlarının satışını, kopyalanmasını, dağıtımını ve kullanımını ifade etmektedir.

Lisans Sözleşmesine Aykırı Kullanma: Tek bir bilgisayar için alınan yazılımın, birden fazla bilgisayarda lisans haklarına aykırı olarak kullanılmasıdır. Yazılım lisansları genellikle tek bilgisayarda kullanmak üzere tanzim edilmektedir. Tek bir bilgisayar için alınan yazılımın lisans hakları çerçevesinde birden fazla bilgisayarda kullanılmak üzere kopyalanması ve çoğaltılması yasaktır.

Lisans Haklarına Aykırı Çoğaltma: Lisans sözleşmesi ile korunmuş bir yazlımın saklanmış olduğu medya ortamının başka bir medya ortamına kanunsuz olarak kopyalanmasıdır. Genel itibariyle ödemeden kaçınmak için daha önce satın alınmış veya yine lisans sözleşmesine aykırı

olarak kopyalanmış yazılımın başka bir medya ortamına taşınmasıdır. Burada söz konusu yazılımı kopyalayan da, kopyalatan da sözleşme ihlali yapmış sayılmaktadır.

Lisans Haklarına Aykırı Kiralama: Değişik medyalar üzerine kayıtlı oyun, film ve yazılımların lisans haklarına aykırı olarak kiralanmasıdır. Başka bir deyişle, oyun, program ve filmleri kiralamaya yönelik özel bir lisans bulunmadan kiralanmasıdır. Uygulamada daha çok film ve oyun CD'lerinin kiralanması olarak karşımıza çıkmaktadır.

1.3.1.3 Diğer Suçlar

Kişisel Verilerin Suistimali: Ticari ya da mesleki sırlar, kişisel bilgileri ya da değerli diğer verileri kişinin kendisine veya bir başkasına menfaat sağlamak ya da zarar vermek amacıyla, bu bilgileri kullanması, satması ve dağıtmasıdır. Daha açık bir ifadeyle, banka, hastane, alışveriş merkezleri, devlet kurumları gibi kuruluşlarda tutulan her türlü kişisel bilginin kişisel menfaat sağlamak veya başkasına zarar vermek amacıyla bu bilgilere sahip kişilerin rızası dışında kullanılmasıdır.

Sahte Kişilik Oluşturma ve Kişilik Taklidi: Hile yoluyla kendisine veya bir başkasına menfaat sağlamak ya da zarar vermek amacıyla gerçek kişilerin taklit edilmesi veya hayali kişilerin oluşturulmasıdır. Bu metotta, gerçek kişilere ait bilgileri kullanarak, o kişinin arkasına saklanılmakta ve o kişinin muhtemel bir suç durumunda sanık durumuna düşmesine neden olunmaktadır. Ayrıca kredi kart numarası oluşturucu programlar gibi araçlar kullanılarak elde edilecek gerçek bilgilerin, hayali kişiler oluşturulmasında kullanılmasıyla menfaat sağlanmakta ve zarar verilmektedir.

Yasadışı Yayınlar: Yasadışı unsurların yayınlanması ve dağıtılması maksadı ile bilgisayar sistem ve ağlarının kullanılmasıdır. Kanun tarafından yasaklanmış her türlü materyalin, web sayfaları, elektronik postalar, haber grupları ve optik medyalar gibi her türlü veri saklanabilecek dijital kayıt yapan sistemler vasıtasıyla saklanması, dağıtılması ve yayınlanmasıdır.[20]

[20] TURHAN Oğuz, Siber Suçlar, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf

1.3.2 Avrupa Konseyi Sınıflandırması

Yıllarca süren tartışmalara ve sınırları aşan sanal çatışmalara rağmen dünya ülkeleri, ulusal sınırlar dışındaki internet zararlarını engellemek ve hukuki açıdan düzenleme yapabilmek için Avrupa Konseyi Siber Suçlar Sözleşmesi ile tek bir anlaşma yapmayı başarmıştır. Avrupa Konseyi'nin hazırladığı Siber Suçlar Sözleşmesi, siber suçlara karşı hukuki açıdan karar alınmasını sağlayan ve taraf olan devletler içinde kararların bağlayıcı olması açısından bu alanda bugüne kadar atılan bölgesel çaptaki en önemli adımdır. 47 ülkeden oluşan Avrupa Konseyi'nde, 2001 senesinde imzalanan ve 2004 senesinde yürürlüğe giren sözleşmeyi, 45 devlet onaylamıştır. Bu sözleşmede amaç "toplumun siber suçlara karşı korunmasına yönelik ortak bir ceza politikası" oluşturmaktır. Böylece üye ülkelerin mevzuatlarını bilişim suçlarıyla ilgili hükümlere uyumlu hale getirmeyi hedeflemişlerdir. Yasadışı erişim ve müdahale, veri ve sistem müdahalesi, cihazların kötüye kullanılması, sahtecilik, sahtekârlık dâhil olmak üzere çeşitli bilgisayar suçlarını yasaklayan yasaların kabul edilmesini gerektiren bir anlaşmadır. Bu anlaşma yalnızca kendi üyeleri için değil diğer devletler için de siber suçlarla mücadelede iyi bir rol model olmuştur.[21]

Avrupa Topluluğu siber suçları dört başlık halinde sınıflandırmaktadır:

1) Verilerin ve bilişim sistemlerinin güvenliğine, bütünlüğüne ve kullanımına ilişkin suçlar,
2) Bilişim suçları,
3) İçerik itibariyle suçlar,
4) Manevi varlığa ve bununla ilgili haklara ilişkin suçlar.

Bu sınıflandırma ile Avrupa Topluluğu,

- Sisteme hukuka aykırı giriş,
- Hukuka aykırı iletişime müdahale,
- Verilerin bütünlüğüne ilişkin fiiller,
- Sistemin bütünlüğüne ilişkin fiiller,
- Bilişim belgelerinde sahtecilik,
- Bilişim sahtekârlığı,
- Bilişim dolandırıcılığı,
- Çocuk pornografisine ilişkin suçlar ve

[21] EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

- Manevi varlığa ve bununla ilgili haklara saldırılar sebebiyle işlenen suçların yaptırım altına alınmasını hedeflemiştir.[22]

1.3.3 Uluslararası Telekomünikasyon Birliği (ITU) Sınıflandırması

ITU siber suçları 4 ana başlık altında toplamıştır. Bunlar:

1) Bilgisayardaki veri ve sistemlerin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı işlenen suçlar (yasadışı erişim, veri çalma, veriye müdahale vb.),

2) Bilgisayar ile ilgili suçlar (online kumar, kimlik hırsızlığı, ücret sahteciliği vb.),

3) İçerikle ilgili suçlar (ırkçılık, nefret söylemi, şiddeti övme, yanlış bilgi vb.) ve

4) Telif hakkıyla ilgili suçlar (telif ve fikri mülkiyet haklarına saldırı)

şeklindedir[23].

1.3.4 McConnel International Sınıflandırması

Verilere Müdahale Edilmesi: Siber uzayda veri transferine müdahale edilmesine ilişkin suçtur. Bu suçun gerçekleşmesi için, verilerin transferi sırasında üçüncü kişilerin bu transfere müdahale ederek veri transferini engellemesi, transferin yönünü değiştirmesi ve üçüncü kişilerin verileri ele geçirmesi gerekmektedir.

Verilerin Değiştirilmesi: Bu suçun oluşabilmesi için verilerin saklı tutulduğu bir ortamda veya iletildiği sırada değiştirilmesi, kısmen veya tamamen tahrip edilmesi gerekmektedir. Buradan çıkan bir sonuç da aktarma sırasında verilerin değiştirilebilir, tahrip edilebilir veya silinebilir olmasıdır. Bu durum iki ayrı suçun işlenmesi durumunu ortaya çıkarmaktadır ve bu halde iki suç birleştirilerek tek bir ceza verilmektedir.

Veri Hırsızlığı: Çalınan verilerin, veri sahibinin veya üçüncü bir kişinin aleyhine olacak şekilde kullanılması veya çalınan veriler sayesinde çalan veya başka biri lehine haksız kazanç sağlanması durumunda ortaya çıkan bir suçtur.

---

[22] KARADAĞ Şerife, Siber Uzayda Uluslararası Hukuk Mümkün mü?, Selçuk Üniversitesi, 2019, http://sssjournal.com/Makaleler/1545056113_06_5-36.ID1522_Karada%c4%9f_2827-2833.pdf

[23] Dr. BAYKARA Muhammet, Siber Suçlar ve Siber Terörizm, http://muhammetbaykara.com/wp-content/uploads/2018/04/3.Hafta-S%C4%B0BER-SAVA%C5%9E-VE-S%C4%B0BER-TER%C3%96R%C4%B0ZM.pdf

Ağ Suçları: Verilerin bir yerden başka bir yere iletilmesini sağlayan ağ sistemine karşı işlenen müdahaleler ikinci suç grubunu oluşturmaktadır. Bu suçlar iki çeşittir.

- **Ağın Engellenmesi:** Ağın tamamına veya bir kısmına erişimin engellenmesidir. Bu suç farklı şekillerde işlenebilmektedir. En sık karşılaşılan şekli web siteleri ve İSS (İnternet Servis Sağlayıcı) üzerinden gönderilen verilere erişimin engellenmesi ya da önlenmesidir. (DDOS -Distributed Denial of Service) saldırılar denmektedir. DDOS saldırılar, "hack" edilen bilgisayarların yönlendirilmiş olduğu siteye, bilgisayar veya sisteme gönderilen veriler nedeniyle başkalarının o siteye, bilgisayara veya sisteme erişiminin engellenmesi veya önlenmesi olarak ifade edilmektedir.
- **Ağ Sabotajı:** Ağın veya sistemin fiziki ve elektromanyetik olarak tahrip edilmesi veya değişikliğe uğratılmasıdır.

Yetkisiz Erişim Suçları: Burada erişimden; sistemin bir kısmına ya da bütününe veya içerdiği verilere ulaşma kastedilmektedir. Bu suç grubunda iki çeşit suça yer verilmiştir.

- **Yetkisiz Erişim:** Sistem içerisindeki mevcut olan bilgilere ulaşma hakkı, söz konusu bilgilere ulaşma yetkisi verilen kişilere aittir. Yetkili kişiler dışında sisteme girip bilgilere ulaşmak ve bunları başkalarıyla paylamak hemen hemen her ülkede suç olarak kabul edilmiştir. Bu suçun hedefi bir bilgisayar sistemi ya da ağıdır.
- **Virüs Yayılması:** Bilişim sistemlerine ağ üzerinden veya manuel olarak CD ve disketler kullanılarak zarar vermek için gerçekleştirilen bir suç fiilidir.

İlgili Suçlar: Bu başlık altında incelenen husus bilişim ve iletişim teknolojileri alanında işlenen suçlarda iştirakin cezalandırılmasıdır. Mevcut ceza kanunlarında iştirak zaten cezalandırıldığından, bu suçlarda ayrıca düzenlemeye gitmenin gereği bulunmamaktadır. Bu başlık altında düzenlenen diğer iki suç türü şunlardır.

- **Bilgisayarla ilgili Sahtekârlıklar:** Kendisine veya başkasına yasa dışı yollarla maddi menfaat sağlamak ve mağduru zarara uğratmak amacıyla, bilgisayar sistemlerinden yararlanarak sahte materyal (banknot, kredi kartı, senet vb.) oluşturmak veya dijital ortamda tutulan belgelerde (formlar, raporlar vb.) değişiklik yapmaktır. Dijital ortamda tutulan dokümanları değiştirmek sahtekârlığın bir çeşidi olup, bilgisayarda mevcut olan belgeler (iş akış programları, personel bilgileri vb.) değiştirilerek insanlarda yanlış kanaat oluşturulabilmektedir.

- **Bilgisayarlarla İlgili Dolandırıcılık:** Haksız fayda sağlamak amacıyla bilgisayar sistemlerine müdahale ederek veya sahte veri girerek veya mevcut bilgileri değiştirerek mağdura zarar verme eylemidir.[24]

1.4 Siber Suçların İşlenme Yöntemleri

Bilişim suçları, klasik suçlarla işleniş amaçları açısından benzerlik göstermekle birlikte, yöntem ve araç açısından farklılıkları bulunmaktadır. Bu tip suçları işlemede araç olarak internet, bilgisayar, pos makinesi, cep telefonu ve diğer çeşitli teknolojik cihazlar kullanılması nedeniyle bu suçlar klasik suçlardan büyük ölçüde farklılıklar göstermektedir. Bilişim suçları klasik suçlar gibi herhangi bir fiziksel mekâna gereksinim duyulmadan herhangi bir bilgisayar veya bir internet ağı üzerinden dünyanın herhangi bir yerinde bu suçlar işlenebilmekte; kişilere, kurum ve kuruluşlara büyük zararlar verilebilmektedir. Bilişim suçu günümüz dünyasında sürekli değişen ve hızla artan herhangi bir fiziki mekâna ihtiyaç duymayan bir suç türüdür. Her an her yerde gerçekleşme durumu vardır.

Bilişim suçlarına konu olan olayların neredeyse tamamına yakını aşağıda belirtilen yöntemlerden biri veya birkaçının birleşimi şeklinde meydana gelmektedir. Yani suçu işleyen kimseler, suçun işlenişi esnasında birden fazla yöntem ve tekniği bir arada kullanabilmektedirler. Bu yöntemler genel olarak bilişim suçları fiilleri içerisinde şu unsurları barındırmaktadır:

- Web sitelerinin homepage (ana) sayfalarını silmek, istedikleri yere yönlendirmek, sayfa yapısı ile oynamak ve bu şekilde internet kullanıcılarını kendi istedikleri sayfalara yönlendirmek,
- Erişime açık sitelerdeki içeriğe sızarak veri kopyalamak suretiyle veri çalmak, bilgi hırsızlığı yaparken ifşa ve deşifre olmamak adına var olan dosyaları değiştirmemek gibi birtakım önlemler almak,
- Erişime açık olan sitelerde tahribat yaratarak bu siteleri saldırılarla kullanılamaz hale getirmek,
- Virüs ve zarar verici benzer yazılımları şahıs ve kurumların bilgisayarlarına yükleyerek zararlar vermek, bu zararlı yazılımlar ile uzak sistemlere erişim sağlayarak fiziksel zararlar vermek, sisteme veya kullanıcıya kalıcı tahribatlar vermek,

[24] KARADAĞ Şerife, Siber Uzayda Uluslararası Hukuk Mümkün mü, Selçuk Üniversitesi, 2019, http://sssjournal.com/Makaleler/1545056113_06_5-36.ID1522_Karada%c4%9f_2827-2833.pdf

- Bilgi hırsızlığı yaparak bir sonraki siber suçunda kullanmak üzere bilgiler elde etmek,
- Sanal ortamı yasal veya yasal olmayan faaliyetlerin propaganda alanı gibi kullanmak veya yasal olmayan faaliyetleri organize ve koordine eden bir merkez haline dönüştürerek kullanmak,
- Farklı yöntemlerle ele geçirerek kendilerine bağladıkları bilgisayarları (zombi veya köle bilgisayar olarak) kullanarak büyük çaplı hizmete erişim engelleme saldırılarında bulunmak,
- Telif hakkı içeren materyallerle ve bilgisayar oyunlarıyla ilgili cracking yaparak yani mevcut yazılım koruma şifrelerini kırarak illegal kullanıma sunmak,
- Sanal ortamı diğer kişilerin haklarını ihlal ederek genel asayiş suçlarını (hakaret, tehdit vs.) işleme yeri olarak kullanmak, sanal ortamı spam amaçlı ve dolandırıcılık amaçlı kullanmak,
- Sanal ortamda çocuk pornografisi üretmek, depolamak, paylaşmak, erişime sunmaktır.

Günümüz dünyasında internetin her an yanımızda ve hayatımızın tam merkezinde olmasından dolayı, insanlara ve kurumlara zarar verici nitelikte yazılımlar her geçen gün artmaktadır[25].

1.4.1 Bilgisayar Korsanlığı: Sistem Güvenliğini Aşarak Erişim Sağlama (Hacking)

Bilgisayar korsanları günümüzde yaygın olarak internet üzerinden diğer bilgisayarlara illegal erişim sağlamaktadırlar. Bu illegal erişimi gerek farklı sistem açığı arama teknikleri, gerekse de farklı zararlı yazılımları programlayarak veya kullanarak sağlamaktadırlar. İllegal erişimi sistem güvenlik uzmanı veya admin (yöneticisi) fark edip müdahale edene kadar hacker, sistemden veri çalma, verileri silme ve sisteme zarar verme türlerinde illegal fiillerde bulunabilmektedir.

Bilişim sisteminin güvenlik duvarının kırılarak sisteme ulaşılması fiilinin yani yaygın tabirle hacking eyleminin en öne çıkan özelliği, bu fiili gerçekleştiren hacker diye anılan şahısların kendi kontrollerinde gerçekleştiriliyor olmasıdır. Yani hacker, fiilin her aşamasında bizzat kendisi bulunarak kendi kontrolünde bu eylemi gerçekleştirir. Bazı durumlarda güvenlik şifrelerinin çözülmesinde teknolojik imkanlar yardımıyla olasılık ve kombinasyon hesaplarını hızlı yapan teknikler kullansalar bile, sistemin içerisine girdikten sonra içeride kontrol

[25] EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

hacker'lardadır. Bu fiil ile yapılan işlemler haberleşme hürriyetine müdahale kapsamında kişilik haklarına karşı yapılan fiillerdir[26].

1.4.2 Oltalama Saldırıları (Phishing Attacks)

Oltalama Saldırıları (Phishing Attacks); bilişim suçu işleyen kişilerin internet kullanıcılarının kredi kartı bilgileri gibi hassas birtakım verilerini ve bilgilerini hazırladıkları sahte bir sayfaya veya çeşitli farklı tekniklerle hazırladıkları sahte siteye kullanıcıları yönlendirerek hassas bilgilerini girmelerini sağlamayı amaçlayan saldırılardır.

Oltalama saldırıları, bilgisayar korsanlarınca günümüzde oldukça yaygın olarak ve son dönemde giderek artan şekilde kullanılan bir yöntemdir. İnternet kullanımının yaygınlaşması ile beraber online bankacılık işlemleri artık bilgisayar hatta mobil uygulamalar aracılığı ile akıllı telefonlar üzerinden kolay ve hızlı şekilde yapılabilmektedir. Ancak özellikle banka internet sitelerinin birebir aynısı yapılarak ve kullanıcıyı bu sahte siteye yönlendirmeye çalışarak işlenen phishing ismiyle uluslararası alanda yaygın olarak kullanılan bu yöntemde ciddi artışlar olmuştur. Bilgisayar korsanları tarafından da phishing yöntemi sıklıkla kullanılmakta ve bunun sonucu hesaba erişen bilgisayar korsanları haksız kazançlar sağlamaktadırlar.

Ayrıca hacker'lar belirledikleri mağdurların e-mail hesaplarını veya kredi kartı bilgilerini ele geçirebilmek için mağdurlara bahse konu hizmeti sağlayan yerden geliyormuş gibi gösterdiği sahte bir form içeren dosyayı mail veya başka yöntemlerle mağdura ulaştırarak, mağdurun formu doldurup göndermesiyle birlikte hassas bilgilere ulaşarak haksız çıkar elde etmektedir. Oltalama saldırılarının büyük çoğunluğu banka hesap bilgilerini ele geçirme amacı gütmektedir. Bu bağlamda hedef kullanıcıların mail hesaplarına bankadan gelen bir e-posta gibi masum gözüken bir mail veya link göndererek akabinde de kullanıcıyı sahte hazırlanmış, ancak gerçekten dışardan bakıldığında bankaya ait internet sitesiymiş gibi gözüken bir siteye yönlendirerek bilgilerini çalmaktadırlar.

Oltalama saldırılarından kurtulmak için, gelen mail ve linkler iyi incelenmeli, şüpheli bağlantılara tıklanmamalıdır. Yanlışlıkla da girilse sitenin URL'si kontrol edilmeli ve kimliği

[26] EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

doğrulanmamış yani "https" bağlantılı güvenli olarak sertifikalandırılmamış sitelere girilmemeli ve kesinlikle kişisel bilgiler paylaşılmamalıdır. Ayrıca bilgisayar programları ve işletim sistemleri güncel olmalı ve güncel bir antivirüs yazılımı kullanılmalıdır[27].

1.4.3 Bilgisayar Virüsleri ve Solucanları (Computer Viruses and Worms)

Bilgisayar virüsleri, bilgisayar kodlama dillerinin imkânlarını kullanarak yazılan ve çeşitli yöntemlerle ağ veya USB bellek tarzı harici depolama birimleri üzerinden diğer bilgisayarlara bulaşan bir tip bilgisayar kodlaması ve programıdır. Virüslere kodlamayla bulaştığı hedef bilgisayarda nereye yerleşeceği ve ne zaman ne yapacağı, hangi verileri sileceği, kopyalayacağı, sisteme ne şekilde zarar vereceği belirlenmektedir. Genel olarak virüsler sisteme zarar verme üzerine kodlanmaktadırlar ve yayılabileceği kadar yayılıp verebileceği kadar çok sayıda sisteme zarar vermeye çalışmaktadırlar. En sık karşılaşılan virüs türü ".exe" uzantılı yani çalıştırılarak kurulan dosyalarla bulaşan türüdür. Bu tür virüsler ".exe" uzantılı dosyalar her çalıştığında sisteme bulaşarak yayılmaktadırlar. Bilgisayarlara virüs bulaşma yöntemleri; e-posta üzerinden bulaşma, indirilen bir program üzerinden bulaşma, tıklanan bir link üzerinden bulaşma, oynanan bir oyun veya izlenen bir videodan sisteme virüs bulaştırma şeklindedir.

Bilgisayar solucanları da bir çeşit bilgisayar virüsü türüdür. Kendisini bir sistemden diğerine kopyalayarak yayılmakta, bunu çok hızlı bir şekilde otomatik olarak yapmakta, bilgisayarın sistemini ele geçirerek kendisini çoğaltmakta ve e-posta vb. uygulamaları kullanarak kendisini başka sistemlere de yaymaktadırlar. Sistemlerin ve sunucuların yavaşlamasına hatta kilitlenmesine yol açarak ciddi zararlar oluşturmaktadırlar. Kendisini ve biraz daha değiştirilmiş kopyasını ağ üzerinden hızlıca dağıtarak kısa sürede çok sayıda sisteme bulaşıp zarar verme amacı taşımaktadırlar. Yayılmak için herhangi bir dosya veya taşıyıcı programa ihtiyaç duymadan bilgisayarın denetimini ele geçirerek, hızlı şekilde yayılmaktadırlar. Sasser solucanı ve Blaster solucanı geçmiş dönemde adı duyulan önemli solucanlardır.

1.4.4 Fidye Amaçlı Yazılımlar (Ransomware)

Günümüzde popüler olan ve özellikle son dönemlerde oldukça sık kullanılan bu yöntem başta büyük kurumlar, şirketler olmak üzere tüm kullanıcıları tehdit etmektedir. Bu yöntemle sisteme

[27] EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

sızan zararlı yazılımı kullanan suçlu, sistemdeki dosyaları ve belgeleri kilitleyerek, belgelerin kurtarılması için mağdurdan ücret talep etmektedir. Bu suçlular genellikle ifşa olmamak için fidyenin, günümüzde oldukça yaygın olarak kullanılan kripto para birimlerinden Bitcoin ve türevi kripto paralar olarak anonim bir hesaba aktarılmasını talep etmektedir. Ancak fidye ödense dahi belgelerin kurtarılması kesin değildir. "Wannacry" ve "Notpetya" son dönem ünlü fidye yazılımlarındandır[28].

1.4.5 Klavye İşlemlerini Kaydeden Program (Keylogger)

Kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırgana gönderen casus yazılımlardır. Klavye işlemlerini kaydeden programlara yaygın kullanım ismiyle keylogger denmektedir. Bu programlar çok küçük programlar olup, çok tehlikelidirler. Klavye işlemlerini kaydedip önceden kodunda belirlenen adrese yollamaktadırlar. Bu durum çok ciddi bir tehlikedir çünkü program yazdığımız her şeyi kaydedip suçlu kişiye göndermektedir. Hem özel hayatımızın gizliliği bağlamında hem de ticari ve bankacılık işlemlerinin güvenliği anlamında çok ciddi tehdit oluşturmaktadırlar. Sadece yazılım olarak değil, klavye altına yerleştirilen bir cihazla da gerçekleştirilebilen bu eylem çok ciddi bir güvenlik zafiyeti yaratmaktadır. İnternet üzerinden kredi kartı bilgilerimizi girdiğimizde bu program tüm bilgileri rahatlıkla kopyalayabilmektedir. Günümüzde bazı şirketler güvenli ödeme yöntemi olarak telefonlara kısa mesaj göndermek suretiyle de daha güvenli bir sistem sunmaktadırlar. Aynı şekilde donanımsal olarak keyloggerlar banka ATM'lerinin klavyelerine de yerleştirilmek suretiyle kredi kartı bilgilerini çalma fiilinde kullanılabilmektedir.

1.4.6 Dağıtık Hizmeti Engelleme Saldırısı (DDOS)

Dağıtık Hizmeti Engelleme Saldırısı, Botnet isimli bir bilgisayar ordusu tarafından belirli bir sunucuya aşırı yüklenme yaparak hizmetin yavaşlamasını veya engellenmesini amaçlayan saldırılardır. Botnet tanımlaması, bot bilgisayarlar, zombi bilgisayarlar veya köle bilgisayarlar olarak isimlendirilen bilgisayarların kurulduğu ağdır. Çok sayıda zombi bilgisayar ile bir veya birden çok sunucuya yüklenerek yapılan saldırılardır. Sunucu bilgisayara Botnet tarafından çok sayıda istek gönderilerek, sunucu işlemez hale getirilmeye çalışılmaktadır.

[28] EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

Botnet yazılımları çeşitli yöntemlerle hedef bilgisayarlara yüklendikten sonra kullanılana kadar pasif bekler ancak kullanıldığı zaman hedef sunucu IP'sine çok sayıda istek göndererek sistemi kilitleyerek, eğer geniş kapasiteli değilse sunucuyu çökertmektedir. Biz farkında olmadan bilgisayarımız bir Botnete dâhil olabilmekte ve bir Botnet saldırısında kullanılabilmektedir. Özellikle bilgisayar başında değilsek ve bilgisayar başında olsak bile bilgisayarımızdan çok sayıda ping diye tabir edilen bağlantı çıkış talebinin farkına varamazsak ne olduğunu anlama imkânımız yoktur[29].

1.4.7 Sosyal Mühendislik Saldırıları

Bilişim suçlarında kullanılmakta olan en etkili yöntemlerden birisi de sosyal mühendislik yöntemidir. Sosyal mühendislik, normal şartlarda insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır. Teknoloji kullanımından çok, insanların hile ile kandırılarak bilgi elde edilmesidir. Sosyal mühendislik yönteminde insanları aldatarak çeşitli bilgiler elde etmek suretiyle sisteme zarar verme, verileri çalma ve sistemi ele geçirme amacı vardır. Oltalama yapma, Spam postalar, telefonla arama ve mesaj gönderme gibi yöntemler en sık kullanılan sosyal mühendislik yöntemleridir.

1.4.8 İstem Dışı Alınan E-Postalar (Spam)

Spam, internet üzerinden çok sayıda kullanıcıya çeşitli içeriklerde kullanıcının istemi dışında genelde tanıtım amaçlı gibi gönderilen mesajlardır. Aynı mesajın çok sayıdaki kopyasının bu tip bir mesajı alma talebinde bulunmamış kişilere, bir nevi zorlayıcı nitelikte gönderilmesi söz konusudur. Spam mailleri gönderen kişilere de spammer denilmektedir.

Spammer olarak adlandırılan bu kişiler elde ettikleri mail adresleri ile bir veri tabanı oluşturarak çeşitli alanlarla ilgili reklam başta olmak üzere çeşitli içeriklerde postalar göndermekte veya bu elde ettiği veri tabanını para karşılığı satmaktadır. Spam, genellikle bir ürünün reklamı, pazarlanması ve pornografik içerikli reklâm ve mesajların dünya çapında kitlelere ulaştırılması amacını taşımaktadır.

[29] EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

1.4.9 Hukuka Aykırı İçerik Sunma

Hukuka aykırı içerik sunma eylemi genel olarak yayınlanması yasak olan müstehcen, kişilik haklarına saldıran, telif haklarını ihlal eden ve çocuk pornografisi içeren içeriğin internet kullanıcılarının erişimine sunulmasıdır. Söz konusu içeriklerin sunulması değişik platformlarda icra edilerek gerçekleştirilmektedir. Hukuka aykırı içerik konusunda dünya genelinde sadece çocuk pornografisi ile ilgili ortak bir görüş vardır. Diğer aykırılıklar ülkelerin mevcut yönetim şekilleri, siyasi yapıları, gelenek ve göreneklerine göre farklılık göstermektedir.[30]

1.4.10 Sık Kullanılan Diğer Yöntemler

Bilişim suçlarını işleme yöntemlerinden en çok bilinenleri detaylı olarak incelenmiş olup, diğer sık kullanılan teknikler de aşağıdadır:

Truva atı yazılımı, internet üzerinden veya e-posta yoluyla bilgisayarlara sızan ve kullanıcı farkına varmadan kendi kendilerine internete bağlı olunduğu anlarda dışarıya veri gönderen programlardır. Çoğunlukla internet üzerinden ücretsiz indirilen yazılımlardaki sistem dosyaları içine, Truva atı yazılımı eklenerek kullanıcılara ulaştırılmaktadır. Bu yazılımı bilgisayarına yükleyen kullanıcı, görünüşte yararlı olan yazılımı bilgisayarına kurduğunda Truva atı yazılımı da kendisini fark ettirmeden çalışmaya başlamaktadır. Truva atı yazılımı kurulmuş olduğu bilgisayarın işletim sisteminin açıklarından yararlanarak bütün sisteme hâkim olmakta ve kendisini gönderen kişinin bütün komutlarını yerine getirmektedir. Bu özelliği nedeniyle faydalı işlerde de kullanılması söz konusudur. Örneğin kurumsal sistem yöneticileri kendi sorumlulukları altında olan bilgisayarlarda meydana gelen arızaları giderebilmek için bizzat kendileri bilgisayarın bulunduğu yere gidemediklerinde, arızası olan bilgisayara trojan programı gönderip bu program sayesinde arızalı bilgisayarın arızasını tespit ederek giderebilmektedirler. Truva atları her ne kadar sisteme zararlı bir yazılım olmaları sebebiyle bilişim virüslerine benzetilebilirlerse de, kendi kendilerine çoğalma özelliklerinin olmaması ve zararsız yazılımmış gibi görünebilme özellikleri nedeniyle bilişim virüslerinden ayrılmaktadırlar.

[30] EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

Mantık bombaları, bilgisayar sistemini şaşırtmak, bozmak veya felç etmek için programlanmaktadır ve bunu gerçekleştirmek içinde, bilgisayara ya mantık dışı ya da yapılan işlemin aksine sürekli bilgi göndermektedir. Mantık bombaları, bilişim sistemlerinde veya ağlarında, daha önceden belirlenmiş özel durumların gerçekleşmesi durumunda zarar verici sonuçlar oluşturmaktadır. Bir mantık bombası, belirlenmiş özel durum gerçekleşene kadar 'Truva atı' programı gibi davranmaktadır. Ancak özel durumun gerçekleşmesinden sonra bilişim sisteminde zararlı etkisini meydana getirmektedir ve bu noktada her zaman kendisini gizli tutmaya çalışan Truva atı programından ayrılmaktadır.

Ağ solucanları, virüs gibi kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır. Bunu otomatik olarak yapmaktadırlar. Bellek veya ağ bant genişliğini tüketmektedirler. Sasser ve Blasser gibi. Ağ solucanları, kullanıcının etkisi olmadan kendi kendine çalışabilen ve aynen kendisi gibi bir kopyasını, veri iletim ağına bağlantısı olan diğer bilişim sistemlerine kopyalayabilen yazılım türlerine verilen genel addır. Ağ solucanları, bir iletişim ağındaki sistemler arasında herhangi bir donanım veya yazılıma zarar verme zorunluluğu olmaksızın dolaşmaktadırlar. Ağ üzerinden bir bilişim sistemine gelen bir ağ solucanı, ya bir virüs gibi davranarak yazılıma zarar verir ya da sisteme bir Truva atı bırakmaktadır. Çoğu zaman ise iletişim ağında çalışan sistem operatörlerine yakalanmamak için bıraktıkları tüm izleri silmektedirler. Solucanlar, bilgisayarın hafızasına yerleşen ve hafıza kısmı yokmuş gibi davranarak sürekli olarak kendilerini buraya yazan yazılımlardır[31].

Tavşanlar, çok hızlı üreyen, kısa zamanda kolonileşerek bilişim sisteminin bilgi işleme gücünü azaltan, bilgisayara veya bilişim sitemine durmaksızın gereksiz işler yapması için komut veren bir yazılımdır. Bunlar, işlemciye sürekli anlamsız komutlar vererek işlemcinin bilişim sisteminin normal işleyişini sağlayan komutlarını vermesini engellemekte ve giderek sistemin yavaş çalışmasını sağlamakta ve en sonunda da sistemi çalışamaz hale getirmektedirler.

Bukalemun denilen ve sistem için normal çalışan, zararsız bir yazılım gibi duran ve onun niteliklerine sahipmiş gibi görünen yazılımlardır ve Truva atlarının yakın akrabalarıdır. Bir bukalemun her defasında çok kullanıcılı bir sistemde kullanıcı adları ve şifreleri için giriş iletilerini taklit edecek şekilde dâhiyane bir şekilde programlanmaktadır. Sisteme giren bütün kullanıcıların adlarını ve şifrelerini gizli dosyaya kaydetmekte, daha sonra sistemin bakım için

[31] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

geçici süre kapatılacağına ilişkin bir mesaj vermektedir. Bu yöntem özellikle bankaların bilişim sistemlerinde gerçekleştirilen hukuka aykırı yarar sağlama suçları için kullanılan etkin bir tekniktir[32].

Gizli Kapılar (Trap Door) tekniği ise, işletim sistemleri veya çok işlevli kullanıcı sistemleri hazırlayan bilgisayar programcılarının bunları meydana getirirken ileride ortaya çıkabilecek durumlara göre, sistem şifrelerinde değişiklik yapabilmeyi veya yeni şifreler girebilmeyi sağlamak üzere sisteme bıraktıkları çeşitli giriş yollarına denmektedir. Bu mekanizmaların, program veya işletim sistemi tamamlandığında ortadan kaldırılması gerekmektedir ancak bazen ya hata sonucu veya ileride kullanılmak amacıyla bu mekanizmalar ortadan kaldırılmamaktadır. Bu gibi durumlarda, bu kapılar kötü niyetli kişilerin yasadışı faaliyetlerine hizmet etmesi amacıyla kullanılmaktadır. Hacking denilen yöntemle, hedefle ilgili keşif yapan korsanlar önemli bilgilere ulaşmakta ve bu verileri kullanarak internet üzerinden eylem gerçekleştirecekleri bilişim sistemine girmektedirler. Bilişim korsanları, ulaştıkları hedef sistemi tarayarak açık portları, işletim sistemini, çalışan servisleri, paylaşılan kaynakları ve kullanıcı isimlerini belirlemektedirler. Bu yolla sisteme sızan sanal korsanlar, bu andan itibaren sistemi çökertmektedirler. Sisteme sızmak için 'hacker'ların kullandığı pek çok yöntem vardır. Şifre kırmak, ağı gözetlemek, oturum çalmak, tampon belleği taşırmak, DOS saldırıları yapmak bu yöntemlerden sadece bazılarıdır.

Çöpe dalma veya artık toplama da denilen bir teknikle, herhangi bir bilgisayar sisteminin çalışmasından geriye kalan veri ve bulguların toplanması işlemi ifade edilmektedir. Bu bilgilerin elde edilme yöntemlerinden ilki, çıktı birimlerince kullanılan ve daha sonra çöpe atılan kâğıt, yazıcı şeridi vb. malzemeler üzerinde kalan bilgilerin toplanması yöntemidir. İkincisi ise bilişim sisteminin belleğinde bulunan ve artık ihtiyaç kalmayan silinmiş bilgiler gelişmiş tekniklerle yeniden elde edilmektedir.

Gizlice dinleme, bilişim sistemlerinin veri naklinde kullandığı ağlara girilerek veya bilişim sistemlerinin yaydığı elektromanyetik dalgalar yakalanarak verilerin tekrar elde edilmesi tekniğidir. Bu teknik bilgisayar ekranlarının yaydığı elektromanyetik dalgaların yakalanması ve tekrar ekran görüntüsüne çevrilmesi suretiyle işlenebileceği gibi bilgisayarlar arasında veri

[32] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

naklinde kullanılan ağlara yapılan fiziksel müdahaleler sonucu, ağda nakledilen verilerin ele geçirilmesi şeklinde de işlenmektedir.

Süper Darbe, bütün kontrolleri geçerek, sisteme müdahale eden programlar olarak tanınmıştır. İş dünyasında kullanılan bilgisayarların çoğunda hırsızlığa karşı bir koruyucu güvenlik sistemi vardır. Sistemin kilitlendiği durumlarda, en kısa zaman içinde yeniden çalışıp işlevsel olabilmeleri için "süper zap" programları kullanılmaktadır: Bu programlar bir yandan sistemdeki çeşitli emniyet tedbirlerini aşarken, diğer yandan da meydana gelen sorunları süratli bir şekilde düzeltmektedir. Tüm güvenlik kontrollerini aşarak, sistemde değişiklikler yapabilmesi bu programın kötüye kullanılmasına neden olmakta ve program kullanıcısına hiçbir güvenlik kontrolüne uğramadan istediği değişiklikleri gerçekleştirme imkânı tanımaktadır.

Bilişim virüsleri, kendi kendini çoğaltma özelliğine sahip, kopyalarını başka sistemlere de bulaştırarak etkileyen yazılımlardır. Bunlar, biyolojik virüslerde olduğu gibi, kendi kendine çoğalıp, bulaşabilme ve sistemi hasta edebilme özelliklerine sahip olarak ve bulaştıkları sistemde bulunan yazılımları çökerterek, bilişim sistemine en fazla zararı verecek şekilde tasarlanmaktadırlar. Sisteme giren virüs hemen ya da zaman ayarlı olarak birkaç hafta veya ay içinde harekete geçmekte; özellikle internet vasıtası ile çok hızlı yayılmaktadır.

Kimlik hırsızlığı/kimlik avı, bir başkasının üçüncü şahısları ve bilgi işlem sistemlerini kendisinin söz konusu kişi olduğuna ikna ederek yanıltmasına, o şahsın çıkarlarına zarar verip kendisine çıkar sağlamasına, ya da bu dolandırıcılığa olanak verecek bilgilere ulaşmasına "kimlik hırsızlığı" veya "kimlik avı" denilmektedir. Kimlik hırsızlarının başlıca yöntemleri: Kimlik kartı, kredi kartı veya banka kartı çalmak, posta kutusundan ya da çöp kutusundan belge çalmak, cep telefonundan ya da bilgisayardan dosya kopyalamak, acil bir telefonmuş gibi arayarak, "annen kaza geçirdi", "arabanız çalınmış", "polis sizi arıyor", vb. şeyler söyleyerek karşıdaki kişinin paniğe kapılmasını sağlayıp kişisel bilgilerini istemek, tam temizlenmemiş eski bilgisayar, eski disk, eski USB bellek ele geçirmek, güvenilir bir web sayfasının (örneğin çalıştığınız bankanın) benzerini kurbana sunup kimlik bilgilerini o yolla vermesini sağlamak, bilgi işlem sistemlerinde korsanlık (hacker) yapmak, kimlik hırsızlığı amaçlı virüs yazıp bulaştırmak, internette kişisel bilgiler aramak ve toplamak, kimlik belge ve bilgilerini başkalarına çaldırtmak, kişisel şifre ve parolaları gizlice izlemek, yüz yüze veya telefonda kişileri kandırıp bilgi almak, namına adres değişikliği kaydettirip belgelerin korunmasız bir

yere gönderilmesini sağlamak, kişinin bilinen bilgilerinden bilinmeyen bilgilerini tahmin etmek, gasp ya da zor kullanarak kimlik bilgilerine ulaşmak, olarak sayılabilmektedir.[33]

2 SİBER GÜVENLİKTE ULUSLARARASI UYGULAMALAR

2.1 Uluslararası Kuruluşların Uygulamaları

2.1.1 Birleşmiş Milletler (UN)

Bilgi güvenliği konusu, 1998 yılında Rusya Federasyonu tarafından Birleşmiş Milletler (United Nations) Genel Kurulu Komitesi'ne konuyla ilgili bir karar taslağı sunulduğundan bu yana BM gündeminde yer almaktadır. Daha sonra Genel Kurul tarafından 53/70 sayılı karar olarak kabul edilmiştir.[34] 1996 yılında Güney Afrika'da gerçekleştirilmiş olan Bilgi Toplumu ve Gelişimi Konferansı ve yine aynı yıl Paris'te düzenlenmiş olan Terörizm konulu konferansta bilgi sistemleri güvenliğine ilişkin alınan kararlara dikkat çekilen bu karar metninde ülkelerin bu alandaki güvenlik tedbirlerini gözden geçirmeleri ve uluslararası çalışmalara katkı sağlamalarına ilişkin beklentiler belirtilmiştir. BM genel kurulu 1998 yılından itibaren her yıl konu ile ilgili bir karar yayınlamıştır. 2002 yılında yayınlanan karar gereği 2004 yılında konu ile ilgili çalışma yapmak için Ülke Uzmanlar Grubu kurulmuştur (A/59/454 Sayılı BM Kararı, 2004). 2004 yılından bu yana, beş Hükümet Uzmanları Grubu (GGE), uluslararası güvenlik bağlamında BİT kullanımının yol açtığı tehditleri ve bu tehditlerin nasıl ele alınması gerektiğini incelemeye devam etmiştir. Bu gruplardan üçü, tüm BM Üye Devletleri tarafından memnuniyetle karşılanan sonuçlar ve tavsiyeler içeren önemli raporlar üzerinde anlaşmaya varmıştır. Ayrıca, her GGE bir öncekinin yaptığı çalışma üzerine inşa edilerek eldeki konularda önemli kümülatif ilerleme kaydetmiştir. BM tarafından çalışmaları öncelikli olarak takip edilen GGE'nin 2015 raporu, 70/237 sayılı kararla oy birliği ile kabul edilmiştir.

2018 yılına kadar benzer bir içerik üzerinden ilerleyen kararlar 2018 yılında değiştirilmiş ve daha kapsamlı bir hal almıştır (A/RES/73/27 Sayılı BM Kararı, 2018). Siber politikaların belirlenmesi, uzmanlar gurubu çalışmaları gibi konuların başlangıç adımları bu kararlar içinde

[33] Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010 https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf
[34] United Nations, RESOLUTION ADOPTED BY THE GENERAL ASSEMBLY https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement

yer almaktadır. Söz konusu kararda bilgi teknolojilerinin ikincil kullanımı vurgulanarak kötü amaçlarla kullanımının her zaman mümkün olduğu belirtilmekte, ülkelerin giderek artan miktarda askeri amaçları için bu teknolojilerden faydalanmaya başladığına dikkat çekilmektedir. Bilgi teknolojileri güvenliğinin sağlanmasında BM'nin liderlik etmesi gerektiği ve ülkeler arası diyalog kurulması konusunda daha çok çaba sarf edilmesi gerektiği tespiti yapılmaktadır.[35]

2.1.2 Uluslararası Telekomünikasyon Birliği (ITU)

Dünya Bilgi Toplumu Zirvesi (WSIS) ve ITU (International Telecommunication Union) Tam Yetkili Konferansının işbirliğine dayanan ITU'nun temel rolü, Bilgi ve İletişim Teknolojilerinin (BİT) kullanımında güven ve güvenlik oluşturmaktır. WSIS'de, Devlet Başkanlarının ve dünya liderlerinin bu alandaki uluslararası işbirliği için bir genel çerçeve olması açısından ITU'nun 2007'de Küresel Siber Güvenlik Gündemi (GCA) ile başlattığı, BİT kullanımında güven ve güvenlik oluşturma uygulayıcısı olarak ITU'yu görevlendirmiştir.[36]

2007 yılında, ITU Genel Sekreteri tarafından başlatılan ITU Küresel Siber Güvenlik Gündemi (GCA), bilgi toplumunda güven ve güvenliği artırmayı amaçlayan uluslararası işbirliği için bir çerçevedir. GCA, işbirliği ve verimlilik için tasarlanmıştır ve ilgili tüm ortaklarla ve bunlar arasında işbirliğini teşvik ederek yapılan çalışmaların tekrarlanmasını önlemek için mevcut girişimlerin üzerine inşa edilmiştir.

2008'de ITU, dünyanın her yerindeki çocuklar için güvenli ve güçlendirici bir çevrimiçi deneyim yaratmaya yönelik çok paydaşlı bir çaba olan Çevrimiçi Çocuk Koruma Girişimi'ni başlatmıştır. Çeşitli ortaklarla iş birliği içinde ITU, politika yapıcılar, ebeveynler, eğitimciler ve çocuklar dahil olmak üzere çeşitli ülkelerde rehberlik sağlamakta ve yeni kapsamlar geliştirmektedir. GCA, Çocukların Çevrimiçi Korunması gibi girişimleri teşvik ederek tüm paydaş gruplarından önde gelen küresel oyuncuların desteğiyle birlikte, dünyanın dört bir yanındaki ülkelere siber güvenlik çözümler bulmaya devam etmiştir.

[35] United Nations, Developments in the field of information and telecommunications in the context of international security, https://www.un.org/disarmament/ict-security/
[36] ITU, ITU Cybersecurity Activities, https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

GCA; yasal tedbirler, teknik ve prosedürle ilgili önlemler, örgütsel yapılar, kapasite geliştirme ve uluslararası iş birliği olmak üzere beş stratejik sütun üzerine inşa edilmiştir. ITU, güvenlikle ilgili uluslararası standartları belirleyen, ülkelerin siber güvenlik stratejilerini belirlemelerine ve bilgisayar olay müdahale ekiplerini kurmalarına yardımcı olan, çocukları çevrimiçi ortamda koruyan, insan kapasitesini geliştiren ve politika diyaloğunu kolaylaştıran küresel bir diyalog platformu olarak hizmet vermektedir.

ITU, siber tehditlere ve siber saldırılara karşı üye devletler arasında ulusal ve uluslararası işbirliğini güçlendirmek için bölgesel ve ulusal siber tatbikatlar yürütmektedir. ITU bugüne kadar 100'den fazla ülkeyi kapsayan siber tatbikatlar gerçekleştirmiştir ve üye ülkelerdeki internet kullanıcıları için güvenli bir alan yaratmak için ITU üye devletlerinin siber güvenliğe olan bağlılığına ışık tutan Küresel Siber Güvenlik Endeksi'ni (GCI) yayımlamaktadır.[37]

2.1.3 Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (IMPACT)

Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (The International Multilateral Partnership Against Cyber Threats, IMPACT), Birleşmiş Milletler destekli ilk siber güvenlik ittifakıdır. IMPACT 2011 yılından bu yana, Birleşmiş Milletlerin BİT uzman kuruluşu olan ITU'nun kilit ortağı olarak hizmet vermektedir.

Siber tehditlere karşı ilk kapsamlı kamu-özel ortaklığı olan IMPACT, küresel topluluğun siber tehditlerle mücadele yeteneklerini geliştirmek için dünya hükümetlerini, endüstriyi ve akademiyi bir araya getiren politik olarak tarafsız bir küresel platform olarak hizmet etmektedir. Şu anda ITU-IMPACT koalisyonunun resmi olarak bir parçası olan toplam 152 ülke ve endüstri devlerinden, akademi ve uluslararası kuruluş ortaklarından gelen güçlü destekle IMPACT, bu alandaki en büyük siber güvenlik ittifaklarından biridir.

Merkezi Malezya'da bulunan IMPACT, ITU'nun Küresel Siber Güvenlik Gündeminin (GCA) operasyonel merkezidir. IMPACT, ITU'nun üye devletlerine siber tehditleri etkin bir şekilde ele almak için uzmanlığa, tesislere ve kaynaklara erişim sağlamanın yanı sıra Birleşmiş Milletler kuruluşlarına BİT altyapılarını korumalarında yardımcı olmaktadır.[38]

[37] ITU, Role of ITU in building confidence and trust in the use of ICTs https://www.itu.int/en/mediacentre/backgrounders/Pages/role-of-ITU-in-building-confidence-and-trust-in-the-use-of-ICTs.aspx

[38] Cooperation Agreement Between INTERPOL and IMPACT on Cooperation in The Field of Cyber Security

IMPACT başlangıçta 'Siber Terörizme Karşı Uluslararası Çok Taraflı İşbirliği' olarak biliniyorken, 2008 yılında IMPACT'ın Dünya Siber Güvenlik Zirvesi'ndeki resmi lansmanı sırasında üye hükümetlerden ve ayrıca IMPACT'ın Uluslararası Danışma Kurulu'ndan gelen geri bildirimlerin ardından, IMPACT'ın adındaki 'Siber Terörizm' kelimeleri daha geniş siber güvenlik rolünü yansıtması açısından 'Siber Tehditler' olarak değiştirilmiştir.

2.1.4 Avrupa Birliği (EU)

Avrupa Birliği (European Union)'nin siber alana ilişkin olarak hayata geçirdiği yasal düzenlemelerin başında 2004 yılında Avrupa Komitesi'nin Siber Suç Sözleşmesi ve Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA)'nın kurulması yer almaktadır. 2005 yılında Bilgi sistemlerinin Korunmasına Yönelik Düzenleme yapılmış ve 2013 yılında Europol (Avrupa Polis Teşkilatı) içerisinde Siber Suçlar Merkezi oluşturulmuştur. 2013 yılında Avrupa Birliği Siber Güvenlik Stratejisi, 2015 yılında Avrupa Birliği Güvenlik Ajandası ve 2016 yılında ise Avrupa Siber Güvenlik Kurumu (ECSO) kurulması faaliyetleri gerçekleştirilmiştir.

Bireysel veya bilgi sistemlerine yönelik saldırıların ardından 2004 yılında İspanya'da gerçekleşen ve yolcu trenlerini hedef alan terörist saldırılar sonrasında Avrupa Komisyonu kritik altyapıların korunmasına yönelik olarak "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunmasına" ilişkin tebliğin yayınlanmasıyla temelleri atılan direktif ile enerji, ulaşım, bilgi teknolojileri ve iletişim sektörüne yönelik düzenlemelere değinmiştir.[39] Kritik altyapılara yönelik saldırılar toplumsal hayatı yakından etkilediği için bu kurumların siber güvenliğinin önemi artmıştır.

2.1.4.1 Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA)

2004 yılında çıkarılan bir düzenleme ile kurulmuş olan AB Ağ ve Bilgi Güvenliği Ajansının (European Union for Network and Information Security, ENISA) merkezi Yunanistan'ın başkenti Atina'dadır. ENISA'nın başlıca görevi, AB içindeki ağ ve bilgi güvenliği sorunlarını önleme ve bunlara yanıt verme yeteneğini artırmak için ulusların hem kendi kapasitelerini hem de birliğin genel kapasitesini geliştirmektir. 2016 NIS Direktifinin ağ ve bilgi güvenliği

https://www.interpol.int/content/download/11270/file/international%20multilateral%20partnership%20against%20cyber%20threats%20IMPACT.pdf

[39] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

hususlarında destek olması için ENISA'ya özel ilave sorumluluklar verilmiştir. ENISA'nın görevleri birliğin organlarını ve üye devletleri bilinçlendirmenin yanında tavsiye ve önerilerde bulunarak veri analizi sağlamaktır.

ENISA, stratejik hedeflere ulaşmak için yönetmeliğe uygun olarak aşağıdaki dört temel görevi üstlenmektedir. Bunlardan ilki Komisyon'a ve üye devletlere ağ ve bilgi güvenliği konusunda gerekli danışmanlığı sağlamaktır. Avrupa'da artan siber güvenlik risk ve saldırıları hakkında veri toplayarak analiz etmesi beklenen ENISA, bu konudaki risk değerlendirmelerini yaparak risk yönetim yöntemlerini de teşvik etmektedir. Son olarak ağ ve bilgi güvenliği konusunda farkındalığı artırarak üyeler arası işbirliğinin güçlendirilmesine katkıda bulunması beklenmektedir.

ENISA'nın bu kapsamda canlı olarak gerçekleştirdiği tatbikatlara katılım sağlayan üye devletler bu tatbikatlar sayesinde ağ ve bilgi sistemlerinin güvenliği tespit edilmekte ve işbirliği ile ilgili olarak ihtiyaçları belirlenmektedir. Aynı zamanda tatbikat sonucunda üyelere bu alanda kendilerini nasıl geliştireceklerine dair öneriler hazırlanmaktadır. Operasyonel açıdan bir gücü olmasa da ENISA; üye ülkelerin siber güvenlik kurumlarının oluşturulmasında ve güvenlik seviyelerinin arttırılmasında aktif ve etkin bir rol oynamaktadır.

2.1.4.2 Avrupa Siber Güvenlik Kurumu (ECSO)

2016 yılında kurulan Avrupa Siber Güvenlik Kurumu (European Cyber Security Organization, ECSO) kendi finans kaynakları olan ve kâr amacı gütmeyen bir kuruluştur. AB içerisindeki siber faaliyetlere ilişkin güvenlik önlemlerini artırmak ve güçlendirmek amacıyla kurulan kurum bu kapsamdaki çalışmaları desteklemektedir. ECSO üyesi kuruluşların içinde büyük şirketler, KOBİ'ler, araştırma merkezleri, üniversiteler, son kullanıcılar, operatörler ve derneklerin yanı sıra AB üye devletlerinin yerel, bölgesel ve ulusal yönetimleri ve Avrupa Ekonomik Alanı (EEA), Avrupa Serbest Ticaret Birliği (EFTA) bulunmaktadır.

ECSO'nun üç ana amacına bakıldığında siber tehditlere karşı Avrupa Dijital Tek Pazarının büyümesinin teşvik edilmesi ve korunması, Avrupa'daki siber güvenlik piyasasının geliştirilmesi ve artan pazar konumu ile rekabetçi bir siber güvenlik ve bilgi ve iletişim teknolojileri endüstrisinin gelişmesinin sağlanması ve Avrupa'nın lider olduğu sektörel

uygulamalarda, güvenilir tedarik zincirlerinin kritik adımları için siber güvenlik çözümlerinin geliştirilmesi ve uygulanmasının yer aldığı görülmektedir.[40]

2.1.4.3 Avrupa Komitesi Siber Suç Sözleşmesi 2004

Avrupa Komitesi'nin Siber Suç Sözleşmesi (EU Cyber Security Act), 2001 yılında üye ülkelerin imzasına açılarak 2004 yılında yürürlüğe giren siber suçlara ilişkin ilk uluslararası antlaşma özelliğine sahiptir. Sözleşmeyi Türkiye, 10 Kasım 2010 tarihinde imzalamış; 2014 yılında ise, buna yönelik olarak 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesine İlişkin Kanun kabul edilmiştir. Bu sözleşme AB üyesi ülkelerin bir araya gelerek hazırladığı ve hazırlandığı yıl da göz önüne alındığında en kapsamlı düzenleme olarak gösterilmektedir. Bu belgeyle kritik türden bilgi ve iletişim altyapısıyla olabilecek saldırılardan ve doğabilecek her türlü zarardan korunması öngörülmüş ve bireylerin bu tür felaketlerden korunmasını amaçlayan tedbirlere başvurulmuştur. Siber saldırılarda yaşanan artışlar nedeniyle kısmi ya da kısıtlı-kapsamlı çalışmalardan sonra daha kapsamlı bir stratejik plan yapılması ihtiyacı doğmuştur.[41]

2.1.4.4 Avrupa Birliği 2013 Siber Güvenlik Stratejisi

2013 yılında AB siber güvenlik politikasının temellerini oluşturacak olan ve Avrupa Ekonomik ve Sosyal Komite ve Bölgesel Komite tarafından hazırlanan "Avrupa Birliği Siber Güvenlik Stratejisi" raporu siber güvenlik kapsamında önemli bir adımdır. Raporda AB'nin siber güvenlik stratejisinin "açık, emniyetli ve güvenli siber ortam" sloganı ile oluşturulması amaçlanmıştır. AB ve uluslararası siber güvenlik politikalarına rehberlik etmesi amacıyla oluşturulan raporda, siber güvenliğin etkin ve etkili bir şekilde sağlanması için siber güvenlik politikalarının temel hak ve özgürlükleri kısıtlamadan uygulanması gerektiği vurgulanmıştır.

AB'nin siber güvenliğe ilişkin dayandığı temel ilkeler incelendiğinde öncelikle fiziksel ortamda sağlanan Avrupa Birliği temel değerlerinin dijital ortamda da oluşturulması ve temel hak ve özgürlüklerin, ifade özgürlüğü ve kişisel bilgilerin ve mahremiyetin korunmasının önemi göze

[40] Avrupa Siber Güvenlik Örgütü https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/european-cybersecurity-organization.aspx
[41] EU Cyber Security Act, European Commission https://digital-strategy.ec.europa.eu/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity

çarpmaktadır. Herkese açık internet ortamının oluşturulması il demokratik ve etkin katılımlı yönetimin oluşturulması diğer önemli ilkeler olarak karşımıza çıkmaktadır.

Bu ilkeler üzerine kurulan 2013 stratejisinde siber esnekliğin sağlanması için, kamu otoriteleri ve özel sektör işbirliği, siber kapasite, kaynak ve verimliliğin geliştirilmesi öngörülmüştür. 2013 stratejisi ile ENISA'nın etkinliği arttırılarak siber güvenliğin sağlanması konusunda daha etkin ve öncü hale getirilmesinin gerekliliği dile getirilmiştir. Bu kapsamda ENISA'nın etkinliği arttırılarak 2013 ve 2017 yılları arasında yaşanan siber saldırıların Avrupa ekonomisine verdiği zararın da beş kat artmasıyla birlikte stratejik plan Eylül 2017'de revize edilmiştir. Revize edilen planda öncelikle Avrupa Siber Güvenlik Araştırma ve Yeterlilik Merkezi'nin kurulması yer almıştır. İkinci olarak acil durumlarda müdahale edilebilmesi için bir mekanizmanın kurulması düşünülmüştür. Siber güvenlik acil durum fonu oluşturulması ve Avrupa savunma fonunun yardımıyla askeri siber güvenliğin bir parçası olacak ortak projelerin geliştirilmesi de diğer iki eylemi oluşturmaktadır. Son olarak ise AB'nin siber saldırılar karşısındaki esneklik, caydırıcılık ve güvenliğinin artırılması hedeflenmektedir. Bu reform hareketinin ortak noktaları, üye ülkelerini katılımı ile operasyonel kurumların oluşturulmaya çalışılması ve siber güvenlik faaliyetlerine yönelik ortak mali fonların kurulmak istenmesi olarak dikkat çekmektedir.[42]

2.1.4.5 Avrupa Birliği 2020 Siber Güvenlik Stratejisi

16 Aralık 2020'de Avrupa Komisyonu ve Birlik Dış İlişkiler ve Güvenlik Politikası Yüksek Temsilcisi yeni bir AB Siber Güvenlik Stratejisi sunmuştur.[43] Yeni Siber Güvenlik Stratejisi, küresel ve açık internetin korunmasını amaçlarken, aynı zamanda sadece güvenliği sağlamak için değil, aynı zamanda Avrupa değerlerini ve herkesin temel haklarını korumak için ekstra tedbirler sunmaktadır. Önceki yılların kazanımlarına da dayanarak, AB eyleminin üç alanında düzenleyici, yatırım ve politika girişimleri için somut öneriler içermektedir. Öncelikle; esneklik, teknolojik egemenlik ve liderlik alanlarına ilişkin olarak Komisyon, kritik kamu ve özel sektör kurumlarının siber dayanıklılık düzeyini artırmak için, Birlik genelinde yüksek düzeyde ortak siber güvenlik için önlemlere ilişkin bir Yönerge kapsamında ağ ve bilgi sistemlerinin güvenliğine ilişkin kurallarda reform yapmayı önermektedir.

[42] CSERNATONİ Raluca, European Union, Time To Catch Up: The Eu's Cyber Security Strategy, 2016 http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cyber-security-strategy/
[43] AB Yeni Siber Güvenlik Yasası, 2020 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

İkinci eylem konusu ise önlemek, caydırmak ve müdahale etmek için operasyonel kapasite oluşturmak alanında öngörülüyor. Komisyon, sivil, kolluk kuvvetleri de dahil olmak üzere siber saldırıları önlemek, caydırmak ve bunlara yanıt vermekten sorumlu AB organları ve Üye Devlet makamları arasındaki işbirliğini güçlendirmek için üye devletlerle ilerici ve kapsayıcı bir süreç aracılığıyla yeni bir Ortak Siber Birim hazırlamaktadır.

Son olarak artan işbirliği yoluyla küresel ve açık bir siber uzayı geliştirmek hedeflenmektedir. AB, önümüzdeki yedi yıl boyunca, özellikle Dijital Avrupa Programı ve Horizon Europe olmak üzere bir sonraki uzun vadeli AB bütçesi yoluyla, AB'nin dijital geçişine eşi görülmemiş düzeyde bir yatırımla yeni Siber Güvenlik Stratejisini desteklemeyi amaçlamaktadır. Bu nedenle üye devletler, siber güvenliği artırmak ve AB düzeyindeki yatırımı karşılamak için AB İyileştirme ve Dayanıklılık Tesisinden tam olarak yararlanmaya teşvik edilecektir. Hedef, başta Siber Güvenlik Yetkinlik Merkezi ve Koordinasyon Merkezleri Ağı olmak üzere AB, üye devletler ve sektörden 4.5 milyar Euro'ya varan birleşik yatırıma ulaşmak ve büyük bir kısmının KOBİ'lere ulaşmasını sağlamak olacaktır.

2.1.4.6 Avrupa Birliği Güvenlik Ajandası (2015)

AB komisyonu tarafından Nisan 2015 tarihinde kabul edilen AB Güvenlik Ajandası (European Agenda on Security) 2015-2020 ile siber suçlar ile daha etkin bir şekilde mücadele edilmesi hedeflenmektedir. Siber suçlarla birlik seviyesinde koordine edilecek ortak tepkilerin verilmesiyle mücadele edilebileceği kabul edilmiştir. Bu kapsamda oluşturulan hareket tarzlarına bakıldığında öncelikle mevcut siber güvenlik önlemlerine yeni bir bakış açısının getirilmesi, yasal düzenlemelerin genişletilmesi ve güncellenmesi amaçlanmaktadır. Siber suçlara yönelik adli araştırmaların geliştirilmesi ve siber suçlar ile mücadele kapasitesinin uluslararası kuruluşlar yardımıyla iyileştirilmesi de Birliğin hedefleri arasındadır.[44]

2.1.4.7 Dijital Tek Pazar Stratejisi (2015)

Mayıs 2015 tarihinde Avrupa Birliği, özel sektör ve kamu kuruluşlarının da katılımı ile Dijital Tek Pazar Stratejisi (Digital Single Market Strategy) hazırlanmıştır. Bu strateji ile Avrupa'da rekabetçiliği teşvik etmek ve siber güvenlik pazarının parçalanmasını engellemek

[44] European Commission, A European Agenda on Security
https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf

amaçlanmaktadır. Üye devletler ile endüstri sektörü arasında güveni sağlamak ve siber güvenlik ürünleri ve çözümleri için talep ve tedarik sektörlerinin dengelenmesine yardımcı olmak hedeflenmektedir. Bu strateji ile Avrupa'da dijital güvenlik endüstrisi kaynaklarının yapılandırılması ve birbirleriyle koordinasyonunda etkili olunması beklenmektedir. Strateji inovatif KOBİ'lerden ürün ve ekipman üreticilerine, kritik altyapı operatörlerine ve araştırma enstitülerine kadar çok çeşitli aktörleri içermektedir. Son olarak ortaklık, siber güvenliğe yapılan yatırımları artırmak için AB, ulusal, bölgesel ve özel kurum ve kaynaklardan yararlanmaktadır. Siber güvenlikte önemli konulardan birisi de kullanılan bilişim ve iletişim sistemlerinin üretiminden itibaren kontrol altına alınması ve dış bağımlılıktan kurtarılarak sistemin güvenliğinin artırılmasıdır. Siber güvenliğin sağlanmasında cihaz ve yazılımlarının üretiminden itibaren kontrol altında bulundurulması ve özellikle sistem açıklarından doğan dış kaynaklı saldırıların azaltılması hedeflenmektedir. Birlik içinde buna zemin sağlayan ve iç kaynaklarından yapılacak her türlü yatırım desteklenmekte ve teşvik edilmektedir.[45]

2.1.5 G-7

Siber güvenlik, özellikle finansal sistemleri siber tehditlerden korumak için işlerin koordine edildiği finans sektöründe G7 üyeleri için kilit öneme sahip bir konudur. G-7'de siber güvenlik konusu ilk olarak 2006 St. Petersburg Zirvesi'nde gündeme getirilmiş olsa da, Japonya'nın 2016 G-7 başkanlığı sırasında siber güvenlik konularına daha fazla odaklanılmıştır. 2016 yılında siber uzayda olduğu kadar dijital ekonomide de güvenlik ve istikrarı destekleyen G7 "Siber İlkeleri ve Eylemleri" benimsenmiştir. Söz konusu belgede arzu edilen siber uzayın tanımı yapılmış, siber uzayda güvenlik ve istikrarın teşvik edilmesine ilişkin beklentiler açıklanmış, dijital ekonominin desteklenmesi gerektiğine yer verilmiş ve bunlara ilişkin G7'nin etkin eylemleri açıklanmıştır.

G-7 eylemleri ile ilgili olarak öncelikle ekonomik büyüme için dijital olarak bağlantılı dünya potansiyelinin en üst düzeye çıkarılması ve küresel zorlukların üstesinden gelmek için işbirliği yapılması taahhüt ediliyor. Dijital uçurumların kapatılması ve yenilikçi iş modellerinin oluşturulmasının yanında yüksek kalitede erişim hizmeti sağlanarak dijital okuryazarlığın artırılması ve dijitalleşmenin benimsenmesi teşvik ediliyor. Ulusların bilgi güvenliği olay müdahale ekiplerinin birbirleriyle yapacakları işbirliğinin teşvik edilmesiyle kapasite geliştirme

[45] Europe Commission, A Digital Single Market Strategy for Europe https://www.politico.eu/wp-content/uploads/2015/04/Digital-Single-Market-Strategy.pdf

ve bilinçlendirme dâhil olmak üzere, siber uzayda güvenliğin ve istikrarın teşvik edilmesi adına işbirliklerinin güçlendirilmesi hedefleniyor. Bir yandan siber güvenlik tehditlerinin paylaşılması ve kritik altyapıların siber güvenlik saldırılarına karşı iyileştirilmesine ilişkin işbirlikleri tavsiye edilirken diğer taraftan siber uzayda güvenlik, mahremiyet ve esneklik konularında araştırma ve geliştirme konularının işbirliği çerçevesinde yürütülmesi taahhüt edilmektedir.[46]

G7 üyeleri, siber uzayda hukukun üstünlüğünü teşvik etme, kapasite geliştirme, güven oluşturma ve siber suçlarla mücadele konularında tüm ülkeleri işbirliğini güçlendirmek için Budapeşte Konvansiyonuna katılmaya davet etmiştir. 2016 Japonya Zirvesinde etkinliğinde yayınlanan Ise-Shima Liderler Bildirgesi, günümüz dünyasında artan önemini yansıtan siber hakkında bir bölüm içermektedir.

2017'de İtalya'da gerçekleştirilen G-7 Zirvesi'nde liderlerce, 2016 G7 Siber İlkeleri ve Eylemlerindeki ifadelerin çoğunu kapsayan Siber Uzayda Sorumlu Devletlerin Tutumuna İlişkin G7 Bildirgesi onaylanmıştır. 2019 yılında Fransa'da gerçekleştirilen Biarritz Zirvesinde ise açık, özgür ve güvenli dijital dönüşüm için bir strateji oluşturulmuştur. Bu belgedeki taahhütler, siber güvenlik alanları da dâhil olmak üzere hibrit tehditlere yönelik yapılan çalışmaların desteklenmesini içermektedir.

2.1.6 Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)

Ekonomik İşbirliği ve Kalkınma Teşkilatı (The Organization for Economic Co-Operation and Development, OECD), 1990'ların başından beri uluslararası işbirliğini kolaylaştırmak için çalışmalar yapan, bu alanda politika analizleri ve önerileri geliştiren bir kuruluştur. Dijital güvenlik konusundaki çalışmaları ile bilgi ve iletişim teknolojilerinin (BİT) yenilikçiliği, rekabet edebilirliği ve büyümeyi destekleme potansiyelini engellemeden güveni güçlendiren politikalar geliştirmeyi ve teşvik etmeyi amaçlamaktır.

OECD, bilgisayar suçları için yönergeler başlatan ilk uluslararası kuruluştur, ancak bugün doğrudan siber suçlar üzerinde çalışmamakta daha çok siber güvenliğe odaklanmaktadır. Kuruluş güven ve güven inşa eden küresel koordineli bir politika yaklaşımını desteklemektedir.

[46] Siberde G7 İlkeleri ve Eylemi, https://eucyberdirect.eu/content_knowledge_hu/g7-principles-and-action-on-cyber/

Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), 2002'de Bilgi Sistemleri ve Ağlarının Güvenliği için yeni yönergeler kabul etmiştir. Kritik bilgi altyapısının korunmasına yönelik bu yaklaşım bir kılavuz olduğu için üye devletler için öneri ve tavsiye niteliğinde olup bağlayıcı değildir.

2004 yılında "İstenmeyen Posta Çalışma Grubu" kurulmuş ve 2006 yılında aynı grup tarafından bir rapor sunulmuştur. 2005 yılında Güney Kore'de ortak bir Bilgi Güvenliği Çalıştayı düzenlenmiş, küresel hükümet olaylarına müdahaleyi teşvik etmek dahil birçok konu tartışılmıştır.

2008 yılında OECD ,"Çevrimiçi Kimlik Hırsızlığına İlişkin Kapsam Belirleme Belgesi" adlı bir proje raporu yayınlamıştır ve Kuruluş bunu önlemek, tespit etmek ve caydırmak için yeterli kanun yaptırımlarının geliştirilmesini tavsiye etmektedir.

2009 yılında OECD, "Bilgisayar Virüsleri ve Diğer Kötü Amaçlı Yazılımlar: İnternet Ekonomisine Bir Tehdit" başlıklı bir kitap yayınlamıştır. Kötü amaçlı yazılım saldırılarının artmasına yönelik olarak kitapta, iyileştirilmiş yasal çerçeveler ve daha güçlü kanun yaptırımı gibi çok çeşitli iyileştirme önerileri yer almaktadır.[47]

2015 yılında yayınlanan "Ekonomik ve Sosyal Refah için Dijital Güvenlik Risk Yönetimi" Tavsiyesi, ekonomik ve sosyal refahı engellemeden dijital güvenliği ele almak için sekiz üst düzey ilke içermektedir. Bu kapsamda genel ilkeler farkındalık, beceriler ve yetkilendirme, sorumluluk, insan hakları ve temel değerler ile işbirliği olarak belirlenmiştir. Operasyonel ilkeler ise risk değerlendirmesi ve çözüm döngüsü, güvenlik önlemleri, yenilik, hazırlık ve süreklilik olarak ele alınmıştır. Söz konusu tavsiye, ulusal stratejiler için rehberlik sağlamaktadır.[48]

OECD'nin 2016 yılında yayınladığı Sağlık Veri Yönetimine İlişkin Tavsiyede, birçok OECD Üyesinin, mahremiyeti korumak, verimliliği sağlamak, kaliteyi teşvik etmek ve yenilikçi araştırmaları teşvik etmek için sağlık verilerinin kullanımı ve paylaşım uygulamalarına rehberlik edecek koordineli bir kamu politikası çerçevesinden yoksun olduğunu kabul

[47] Bilgi Güvenliği ve Gizlilik Politikasına İlişkin OECD Kaynakları https://www.oecd.org/sti/ieconomy/security-and-privacy-resources.htm
[48] OECD Dijital Güvenlik Risk Yönetimi Raporu, 2015 https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

edilmektedir. Temel amaç, tarafların sağlıkla ilgili kamu yararına hizmet etmek için kişisel sağlık verilerinin mevcudiyetini, kullanımını ve aynı zamanda mahremiyetin, kişisel sağlık verilerinin ve veri güvenliğinin korunmasının teşvik edilmesi için bir ulusal sağlık verileri yönetim çerçevesi oluşturulmasının ve uygulanmasının tavsiye edilmesidir.[49]

OECD'nin dijital güvenlik alanında birçok güncel çalışması bulunmakta, ülkelerin bilgi güvenliği stratejilerinin geliştirilmesinde, ülkeler arasında işbirliğinin sağlanmasında ve geliştirilmesinde büyük rol oynayan kuruluş, bağlayıcı olmayan tavsiye niteliğindeki çalışmaları ve örnek raporlarıyla, siber güvenlik alanındaki çalışmalara da ışık tutmaktadır.

2.1.7 Küresel Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST)

Küresel Olay Müdahale ve Güvenlik Ekipleri Forumu (Forum of Incident Response and Security Teams, FIRST), üye ekiplerle birlikte olay müdahale ekiplerinin en iyi uygulamalara, araçlara ve güvenilir iletişime erişim sağlayarak güvenlik olaylarına daha etkin bir şekilde yanıt vermesini sağlamak amacıyla kurulan, kâr amacı gütmeyen bir kuruluştur. FIRST çerçevesinde, bilgisayar olay müdahale ekipleri bilgisayar güvenliği olaylarını işbirliği içinde ele almakta ve olay önleme programlarını teşvik etmektedir. Ekip üyeleri ayrıca teknik bilgileri, araçları, metodolojileri, süreçleri ve en iyi uygulamaları geliştirerek paylaşmakta ve daha emniyetli ve daha güvenli bir küresel elektronik ortamı teşvik etmek amacıyla işbirliği yapmaktadır.

FIRST tarafından üstlenilen faaliyetlerde; kaliteli güvenlik ürünlerinin, politikaların ve hizmetlerin geliştirilmesinin teşvik edilmesi, en iyi bilgisayar güvenliği uygulamalarının geliştirilmesi ve dünyanın dört bir yanındaki kuruluşlardan gelen göstergelerle müdahale ekiplerinin oluşturulması ve genişletilmesinin teşvik edilmesi amaçlanmaktadır.

FIRST, harici standart geliştirme çalışmalarına da katkıda bulunarak ve üyelerin kuruluş içinde standartlar geliştirmesini ve yayınlamasını teşvik ederek, üyelerin olay müdahale süreçlerini ve etkinliklerini standartlaştırmasına yardımcı olmak için çalışmaktadır. Kuruluş ayrıca, eğitim ve burs programı aracılığıyla kapasite geliştirme faaliyetleri yürütmektedir. Ayrıca, İnternet Yönetişim Forumu (IGF) gibi internet yönetim süreçlerine esas olarak içerik, en iyi uygulamalar ve güvenlik ekiplerinin rolü hakkında bilgi sağlayarak katılmaktadır.

[49] Konseyin OECD Yasal Enstrümanları Sağlık Veri Yönetimine İlişkin Tavsiyesi https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf

FIRST, herkes için güvenli bir internet sağlamak için dünyanın her ülkesinden olay müdahale ve güvenlik ekiplerini bir araya getirmeyi ve olayların önlenmesinde işbirliği ve koordinasyonu geliştirmeyi, olaylara hızlı tepki vermeyi ve üyeler ve genel olarak topluluk arasında bilgi paylaşımını teşvik etmeyi amaçlamaktadır.[50]

2.1.8 Uluslararası Polis Teşkilatı (INTERPOL)

Siber uzayda sınırın olmaması, tehditlerin ve saldırıların herhangi bir zamanda herhangi bir yerden gelebilmesi polis için zorluk yaratmaktadır; çünkü olaylar şüphelileri, mağdurları ve birden fazla ülkeyi kapsayan suçları içerebilmektedir. INTERPOL (The International Criminal Police Organization), üye ülkelerin siber tehditlere yanıt vermelerini belirlemelerine, öncelik sırasına koymalarına ve koordine etmelerine yardımcı olmaktadır. Tehditler, eğilimler ve riskler hakkında güncel verileri paylaşan özel siber güvenlik ortaklarıyla işbirliği yaparak, polisin eylemlerini yönlendirmek için en ilgili güncel tehdit bilgilerine sahip olmasını sağlamaktadır. Bu verileri, gelişmekte olan tehditlere hazırlanmak için tahminler yaparken, en acil tehditlerin belirlenmesi için önleyici stratejileri geliştirmede ülkelere yardımcı olmak adına siber istihbarat oluşturmak için kullanmaktadır.

Bünyesindeki Siber Füzyon Merkezi ile ülkelere tutarlı, eyleme geçirilebilir istihbarat sağlamak için siber uzaydaki suç faaliyetleri hakkında mevcut tüm bilgileri toplamak ve analiz etmek için kolluk kuvvetleri ve endüstriden siber uzmanları bir araya getirmektedir. Siber Füzyon Merkezi ülkeleri yeni, yakın veya gelişen siber tehditlere karşı uyarmak için raporlar yayınlamaktadır. Yayınlanan raporlar kötü amaçlı yazılım, kimlik avı, güvenliği ihlal edilmiş devlet web siteleri, sosyal mühendislik sahtekârlığı ve daha fazlasını içeren belirlenmiş tehditleri kapsamaktadır. 2017'den beri 150'den fazla ülkede polise 800'den fazla ihbarda bulunulmuştur.

2017 yılında yayınladığı Küresel Siber Suç Stratejisi ile 2016-2020 yılları arasında özel polislik yeteneklerini koordine ederek ve sunarak üye ülkelerin siber suçla mücadele çabalarını destekleme planını özetlemektedir. INTERPOL'ün Siber Suç Programının birincil kapsamı, genellikle kötü amaçlı yazılım yoluyla bir cihaza yetkisiz erişim elde etme amacıyla veya meşru bir kullanıcıya erişimi engellemek gibi bilgisayarlara ve bilgi sistemlerine karşı işlenen suçları

[50] Position paper on cybersecurity developments within the UN context https://www.dfat.gov.au/sites/default/files/cyber-submission-first-forum-for-incident-response-and-security-teams.pdf

hedeflemektir. Ancak INTERPOL, bilgisayar ve bilgi sistemlerinin kullanımının mali dolandırıcılık ve sosyal medyanın terörist kullanımı gibi suçları artırdığı durumlarda siber destekli suçlarla mücadelenin öneminin farkındadır.[51]

Siber Suç Programı, Singapur'daki çok paydaşlı Siber Füzyon Merkezi, Dijital Adli Tıp Laboratuvarı ve İnovasyon Merkezi ile donatılmış INTERPOL Küresel İnovasyon Kompleksi tarafından yürütülmektedir.

INTERPOL'ün kurduğu "INTERPOL Daha Güvenli Bir Dünya Vakfı" merkezi Cenevre'de bulunan kar amacı gütmeyen bir kuruluştur. Vakıf, stratejik küresel ortaklıklar kurarak INTERPOL ve diğer kurumları desteklemekte, siber suçlar da dâhil olmak üzere birçok alanda finansal destek sağlamaktadır. Singapur'daki Siber Füzyon Merkezi de bu kapsamda eyleme geçirilebilmesi olası siber istihbaratları elde etmek, analiz etmek ve yaymak için mevcut ulusal kapasiteleri artırmak adına faaliyet göstermektedir.[52]

2.2 Ülkeler

2.2.1 Amerika Birleşik Devletleri (ABD)

Amerika Birleşik Devletleri, internet ve bilgisayar alanındaki birçok teknolojik gelişmeye öncülük etmek ve gelişimi için gerekli zemini hazırlamakla birlikte teknolojinin getirdiği güvenlik açıklarıyla ilgili olarak, 2003 yılında yayımladığı ilk ulusal siber güvenlik stratejisi olan "Güvenli Siber Uzay" belgesi ile dünya çapında siber güvenlik politikası ve stratejisi geliştirme konusunda öncü olmuştur.

2003 yılında yayınlanan bu belgenin dışında siber güvenlik politikası üzerine ulaşılabilir diğer belgeler 2011, 2013 ve 2015 yıllarında yayınlanmıştır. 2011 yılında yayınlanan siber güvenlik strateji belgesi beş adet stratejik öncelikten oluşmaktadır. Bunlar, savunma departmanının organizasyonel olarak geliştirilmesi, yeni savunma içeriklerinin edinilmesi, kamu-özel işbirliği, diğer ülkelerle bu konuda güçlü ilişkiler kurulması ve yaratıcılığın artırılmasıdır.

[51] Cybercrime threat response, INTERPOL https://www.interpol.int/Crimes/Cybercrime/Cybercrime-threat-response
[52] INTERPOL Foundation for a Safer World, INTERPOL https://www.interpol.int/Our-partners/INTERPOL-Foundation-for-a-Safer-World

2013 yılında ise ABD Savunma Bakanlığı, "Savunma Departmanı Ağları, Sistemleri ve Bilgiyi Savunma Stratejisi" isminde bir belge yayınlamıştır. Akabinde 2014 yılında Beyaz Saray'da ABD ile AB arasında siber güvenlik iş birliğine dair bir yazılı açıklama yapılmıştır. Bu konudaki söz konusu iş birliği; internet yönetişimi, internet özgürlüğü, siber uzayda insan haklarının korunması gibi konu başlıklarını kapsamaktadır.

ABD Savunma Bakanlığı, "Siber uzay harekatları için Ulusal Askeri Stratejisi" ni yayınlayarak siber uzayı bir savaş alanı olarak algıladığını göstermiştir. Bu belgede siber uzay; veri saklamak, değiştirmek, ağ sistemleri ve ilgili fiziksel altyapılar sayesinde veri akışını sağlamak için elektronik ve elektromanyetik spektrumun kullanıldığı bir alan olarak tanımlamaktadır.

ABD Savunma Bakanlığı'nın son olarak 2015 yılında yayınladığı diğer bir belge ise "Siber Strateji" (Cyber Strategy) ismini taşımaktadır. Daha genel bir ifade kullanılan bu belge strateji olarak da daha kapsayıcıdır. Belge ile yeni bir siber strateji ön görülmekle birlikte stratejiye yönelik atılan somut adımların da altının çizildiği görülmektedir. Belge yeni bir siber stratejinin gerekliliği olarak üç durumdan bahsetmektedir. Birincisi ABD çıkarlarına, savunma ağlarına ve bilgi sistemlerine karşı artarak devam eden kapsamlı saldırılar; ikincisi, dönemin başkanı Obama'nın Savunma Bakanlığına diğer Birleşmiş Milletler (BM) ülkeleriyle birlikte hareket ederek bir savunma planı oluşturma direktifi ve son olarak da 2012 yılından itibaren Savunma Bakanlığının oluşturmaya başladığı ve kurumun görevlerini yerine getirmek üzere operasyonları yürütecek olan, sivil ve askeri yaklaşık 6.200 personelden oluşan Siber Görev Güçleri olarak ifade edilebilir. Bu yönleriyle 2015 yılında yayınlanan strateji belgesi, önceden de altı çizildiği üzere, somut adımlara önem vermiştir. Bu doğrultuda diğer belgelerde belirtilen stratejik hedeflerin dışında bu belgede, stratejik hedeflere ulaşılması için gerçekleştirilen uygulamalara da yer verilmektedir.[53]

ABD'nin siber güvenlik stratejileri; kritik altyapılara karşı siber saldırıların önlenmesi, siber saldırılara karşı ulusal güvenlik açıklarının azaltılması ve siber saldırılardan gelecek zararın minimuma indirilmesi olarak üç ana başlıkta değerlendirilebilmektedir.

Ülkede bu alanda birçok kurum ve kuruluş tarafından yürütülen çalışmalar bulunmaktadır. ABD'de siber güvenlik çalışmaları Merkezi İstihbarat Teşkilatı (Central Intelligence Agency,

[53] Cyber Strategy, Department Of Defense, United States Of America
https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

CIA), İç Güvenlik Bakanlığı (DHS, Department of Homeland Security) ve Savunma Bakanlığı (Department of Defense, DOD) tarafından takip edilmekte ve gerekli bilgi paylaşımı ve farkındalık sağlanmaktadır. Ancak 2018 yılında kabul edilen Siber Güvenlik ve Altyapı Güvenliği Ajansı Yasası ile birlikte kurulan Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), kritik hizmetleri ve Amerikalıların mevcut yaşam düzenini korumak için siber ekosistemin güvenliğini, dayanıklılığını ve iş gücünü güçlendirmek için ülkenin stratejik ve bütün halinde çalışmasına liderlik etme görevini üstlenmiştir.[54]

Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) bünyesinde yer alan Ulusal Risk Yönetim Merkezi (NRMC), ülkenin kritik altyapısına yönelik en önemli riskleri belirleyerek bu risklerin yönetimine rehberlik etmektedir. CISA, siber saldırılara karşı savunma için mevcut kapasiteyi geliştirmek ve ortak paydaşların ve kurumların temel işlevlerini destekleyen ".gov" ağlarını korumak için siber güvenlik araçları, olay müdahale hizmetleri ve değerlendirme yetenekleri sağlamak için federal hükümetle birlikte çalışmaktadır.

2.2.2 Almanya

Almanya'nın siber güvenlik stratejisi yaklaşımı önceden sivil bir önleyici yaklaşım iken günümüzde daha kapsamlı bir hale gelerek stratejik askeri yönleri içermeye başlamıştır. Alman siber güvenliğinin gelişimi üç aşamada düşünülebilir. İlk aşama (1991'den 2011'e kadar), kritik bilgi altyapısının korunması bağlamında siber güvenliğin stratejik bir konu olarak ortaya çıkışını işaret etmektedir. İkinci aşamada (2011'den 2016'ya), hükümet 2011'de ilk ulusal siber güvenlik stratejisini kabul ettikten sonra mevcut politikaları da konsolide etmiştir. Almanya, 2016'dan 2018'in başına kadar olan üçüncü aşamada, siber güvenliğe kapsamlı bir yaklaşımın yanı sıra hibrit bir savaşta siber güvenliğin stratejik askeri boyutunu ilk kez vurgulayan ulusal bir savunma stratejisinin ana hatlarını çizen ikinci ulusal siber güvenlik stratejisini benimsemiştir.

İlk aşamada (1991–2011) Almanya'da siber güvenlik politikası veri koruma ve BT güvenliğinin teknik veya organizasyonel yönleriyle ilgili olmuştur. 1991 yılında, Federal Bilgi Güvenliği Ofisi'ni (Bundesamt für Sicherheit in der Informationstechnik, BSI) kuran yasanın kabul edilmesiyle BSI tarafından yürütülen bir dizi kritik altyapı çalışmasının ardından, 2005'te

[54] PERNIK Piret, WOJTKOWIAK Jesse, KIRSS Alexander Verschoor, National Cyber Security Organisation: United States, https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf

Ulusal Bilgi Altyapısı Koruması Planı (NPSI) yürürlüğe konmuştur. NPSI, Almanya'daki BT güvenliğiyle ilgili ilk ulusal stratejidir ve esas olarak üç stratejik hedefle; önleme, hazırlık ve sürdürülebilirlik, ülkenin BT'ye bağlı altyapılarının güvenliğini güçlendirmeye odaklanmaktadır. 2007'de kritik altyapıların korunması planlarının oluşturulmasına dair ilk kapsamlı stratejisini oluşturmuştur. Genel olarak, NPSI, 2011'den sonraki siber güvenlik politikaları ve Alman ulusal siber güvenlik stratejisi için zemin hazırlamıştır.

2. Aşama (2011–2016)'da Almanya ilk olarak Ulusal Siber Güvenlik Stratejisini (NCSS) kabul etmiştir. NCSS, siber güvenlik politikasının kapsamını teknik altyapıya özgü olmaktan, dijital alanda gerçekleşen ekonomik, sosyal ve kültürel etkileşimleri içeren toplumsal stratejik bir konuya doğru genişletmektedir. NPSI gibi, NCSS'nin genel bir yol gösterici ilkesi, kamu ve özel paydaşların ortak olarak hareket etmeleri ve koruma görevlerini birlikte yerine getirmeleri gerektiğini vurgulayan bir ulus yaklaşımıdır.

Stratejide temel olarak kritik bilgi altyapılarının korunması, Almanya'daki BT sistemlerinin güvenli hale getirilmesi, kamu yönetiminde BT güvenliğinin güçlendirilmesi, Ulusal Siber Müdahale Merkezi ve Ulusal Siber Güvenlik Konseyi'nin kurulması, siber uzayda etkili suç kontrolü, Avrupa'da ve dünyada siber güvenliği sağlamak için yeterli işbirliğinin sağlanması, güvenilir bilgi teknolojilerinin kullanılması ve siber saldırılara yanıt vermek için gerekli olan araçların temini maddeleri göze çarpmaktadır.

Ancak kontrol mekanizmasına bakıldığında hükümetin ulusal bir siber müdahale merkezi ve ulusal bir siber güvenlik konseyi kurmasına rağmen bunda başarılı olamadığı, kurumlar arası işbirliği mekanizmalarına sahip kapsayıcı, etkili bir ulusal siber güvenlik mimarisinin henüz olgunlaşmadığı, siber saldırılara yanıt vermek için kapsamlı sürdürülebilir araç geliştirilmesi belirsizliğinin korunduğu gözlemlenmiştir. Siber güvenlik politikalarını uygulamak için yetkin personelin eksikliği, günümüzde de siber güvenlik politikasındaki en büyük zorluklardan biri olarak devam etmektedir.

2015 yılında kabul edilen "Bilgi Teknolojileri Güvenlik Yasası" ile birlikte kritik altyapıların korunması ve iyileştirilmesi yolunda ciddi bir adım atılmıştır. Yasa ile yedi sektördeki (enerji, sağlık, bilgi ve telekomünikasyon teknolojileri, ulaşım, su, gıda ile finans ve sigorta sektörleri) kritik altyapı operatörlerine çeşitli yükümlülükler getirilmiştir. Bu hususta enerji, su, gıda ve

BİT sektörleri için Mayıs 2016'da, sağlık, finans, sigorta, ulaştırma ve lojistik sektörleri için 2017'de ilgili yönetmelikleri yayınlanmıştır.

3. Aşama (2016–2018) ise Kasım 2016'da, Alman federal hükümetinin ikinci ulusal siber güvenlik stratejisini kabul etmesiyle başlamıştır. Aynı yıl hükümet ikinci ulusal savunma stratejisi olan "Alman Güvenlik Politikası ve Silahlı Kuvvetlerin Geleceği Hakkında Beyaz Kitap" ı onaylayarak ilk kez özellikle siber güvenliğin stratejik askeri yönleri ana hatlarıyla belirlenmiştir. Beyaz Kitap, Alman Silahlı Kuvvetlerinin hızla küreselleşen, yüksek teknolojili bir tehdit ortamına verdiği yanıt olarak ortaya çıkmakla birlikte içeriğinde fiziksel hasara neden olabilecek siber saldırıların yanı sıra, kamuoyunu etkilemek için dijital iletişimin kullanılması, sosyal medya ve haber portallarındaki bilgilerin manipüle edilmesiyle yapılabilecek dezenformasyon kampanyalarının çoğulcu toplumlar için ciddi bir zorluk olduğundan bahsedilmektedir.

İkinci Ulusal Siber Güvenlik Stratejisi, ilk stratejiye kıyasla, stratejik hedefleri, araçları ve eylem öğelerini daha tutarlı ve yapılandırılmış bir şekilde ana hatlarıyla belirtmektedir. Savunma Bakanlığı 2011 stratejisine göre daha fazla katılım gösterdiği stratejide dört eylem alanı özetlenmektedir:

- Sayısallaştırılmış Bir Ortamda Güvenli ve Kendi Kendine Belirlenmiş eylem alanı ile, siber güvenliğe kullanıcı merkezli bir bakış açısı benimsemekte, dijital okuryazarlığın geliştirilmesini, farkındalık yaratmayı, güvenli e-kimlikleri ve yanı sıra, BİT'lerin güçlendirilmiş sertifikasyonu ve onayını ve bir BT güvenliği "kalite etiketinin" uygulanmasını teşvik etmektedir. Böyle bir etiket, tüketicilerin ve küçük ve orta ölçekli işletmelerin BT ürünlerinin güvenliğini değerlendirmesini kolaylaştırarak BT'ye olan güveni güçlendirmelidir. Bu bölüm aynı zamanda toplum genelinde dijital inovasyonun nasıl güvenli bir şekilde tasarlanabileceğini de özetlemektedir.
- Devlet ve Sanayinin Ortak Çabası eylem alanı ile strateji, güvenilir kamu-özel sektör işbirliğine duyulan ihtiyacı vurgulamakta, Alman bilgi teknolojileri endüstrisini güçlendirmek için endüstriyel politika önlemlerini savunmakta ve daha fazla BT güvenlik personeli yetiştirerek mevcut kaynakları verimli bir şekilde kullanmayı hedeflemektedir. İlk kez bir NCSS, istihbarat ve polis teşkilatları için saldırı kabiliyeti geliştirme planlarını şeffaf bir şekilde ana hatlarıyla açıklamaktadır.
- Etkili ve Sürdürülebilir Bir Siber Güvenlik Mimarisi eylem alanı ile strateji, ulusal siber güvenlik mimarisindeki bazı eksikliklere değinmekte ve daha iyi koordinasyon ve siber

savunma etkinliğinin artırılması için önlemler önermektedir. Polis teşkilatları ve iç istihbarat hizmetleri için bilgisayar korsanlığı araçları da dahil olmak üzere siber yetenekler geliştirecek olan güvenlik alanında BT için bir merkez ofisinin kurulacağı da ifade edilmektedir.

- Almanya'nın Avrupa ve Uluslararası Siber Güvenlik Politikası Tartışmalarında Aktif Konumlanması eylem alanı ile stratejide, siber güvenliğin uluslararası diplomatik boyutu önemli bir stratejik öncelik haline gelmiştir. Hükümet, etkili bir Avrupa siber güvenlik politikasını aktif olarak şekillendirmeyi, NATO siber savunma politikasını daha da ilerletmeyi ve organizasyona aktif olarak katılmayı hedeflediğini ilan etmektedir.

2005 yılından bu yana, Alman hükümeti siber güvenlik stratejisini sürekli olarak güncellemiş olup son strateji ile hemen hemen tüm ilgili eylem alanlarını kapsamaktadır. 2016 NCSS, 2011'deki ilk NCSS'den daha geniş bir kapsama sahipken, stratejik bir programdan ziyade ilgili federal hükümet kurumları için bir çalışma programı oluşturmaktadır. Hedefleri ve eylemleri ana hatlarıyla belirtir, ancak açık sorumluluklar belirtmez ve hedeflerin uygulanması için ölçülebilir kaynaklar tahsis etmez. Başarıların değerlendirilebileceği somut ölçülebilir hedeflerden yoksundur. 2018 koalisyon hükümet anlaşması temelde, hükümet için araştırma-geliştirme ve BT ürünlerinin güvenliğinin artırılması alanındaki mevcut eylem çizgilerini tamamlayan çeşitli eylem alanlarının ana hatlarını çizmektedir. BT güvenliği alanında araştırma ve geliştirmeyi, yetkinlik merkezleri kurmayı, güvenli elektronik kimlik ve uçtan-uca şifreleme çözümlerini vatandaşlar için daha kolay erişilebilir hale getirmeyi vaat etmektedir. İnternet bağlantılı ürünler için minimum BT güvenlik standartlarını endüstri ile işbirliği içinde geliştirmeyi ve tüketiciler için BT ürünlerinin güvenlik düzeyini gösteren bir kalite etiketi sunmayı amaçlamaktadır. Kurumsal açıdan, BSI'nin siber güvenlikteki rolünü güçlendirmeyi ve endüstri ile kamu otoriteleri arasındaki güvenilir işbirliğini geliştirmek için endüstri ile yeni bir siber ittifak oluşturmayı amaçlamaktadır. Bu nedenle, koalisyon anlaşması, Almanya'da BT'nin teknik koruma düzeyini artırma potansiyeline sahip bir dizi gerekli BT güvenlik önlemi sunmaktadır.[55]

[55] Almanya Siber Güvenlik Stratejisi https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?_blob=publicationFile

2.2.3 Fransa

Fransa, 2008 yılında ülkenin karşı karşıya olduğu tehditleri belirleyebilecek ve bu tehditle yüzleşmek için savunma ve ulusal güvenlik üzerine gerekli yetenekleri tanımlamaya yardımcı olacak bir Beyaz Kitap'a ihtiyacı olduğuna karar vermiştir. Ulusal altyapılara yönelik bir siber saldırı riskinin sonraki on beş yılın olası en büyük tehditlerinden biri olduğuna dikkat çeken 2008 Beyaz Kitabı, bu tür saldırıların ülke üzerindeki etki potansiyelinin büyüklüğüne dikkat çekiyor. Beyaz Kitap ayrıca bilgi toplumunun gelişmesi ve devletin ve toplumun temel süreçlerinde bilgi teknolojilerinin giderek daha yaygın bir şekilde kullanılmasıyla bilgi teknolojilerinin süreçlerine olan bağımlılığımızın sürekli arttığını vurguluyor.

2008 yılında yayınlanan Beyaz Kitap, devleti siber saldırıları önleme ve bunlara yanıt verme kapasitesini geliştirmeye ve bunu ulusal güvenlik teşkilatının ana önceliği haline getirmeye çağırmıştır. Spesifik olarak, siber savunma alanında, siber saldırılar için erken tespit kabiliyetine ve bir organizasyonun en basit olanından en geniş kapsamlısına kadar çeşitli saldırılara karşı koyabilme ihtiyacını vurgulamıştır.

Savunma ve ulusal güvenlik üzerine Beyaz Kitap'ın önerileri doğrultusunda Fransa Ulusal Siber Güvenlik Ajansı (ANSSI) oluşturulmuştur. Ulusal bir siber güvenlik stratejisi önermek için ANSSI'nin kuruluş kararnamesi ile siber güvenlik için stratejik bir komite kurulmuştur. Bunun yanı sıra Beyaz Kitap, ulusal bölgedeki her savunma ve güvenlik alanı için bölgesel bir siber güvenlik gözlemevi yerleştirmiştir. Bu gözlemevlerinin amacı, siber güvenliği geliştirmek için alınan önlemlerin ülke çapında yaygınlaştırılmasıdır.

Şubat 2011'de Fransa Ulusal Siber Güvenlik Ajansı (ANSSI)'nın yayınladığı Siber Savunma ve Siber Güvenlik Stratejisi, siber saldırılara karşı korunmak ve savunmak ve siber uzayda Fransız vatandaşlarının, işletmelerinin ve ulusunun güvenliğini sağlamak için dört stratejik hedef ortaya koymaktadır.

Öncelikle kendi özerkliğini korurken, sahadaki diğer büyük ulusların da merkezinde yerini alarak siber savunmada küresel bir güç olunması hedeflenmiştir. İkinci olarak bağımsızlık ilkesini koruyarak Fransa'nın karar almadaki özgürlüğünün muhafaza edilmesi ve üçüncü olarak da ulusal kritik altyapıların siber güvenliğinin desteklenmesi yer almaktadır. Son olarak siber uzayda güvenliği sağlamak hedeflenmiştir. Bu dört stratejik hedefi ve bunlardan

kaynaklanan yedi çalışma alanını belirleyen belge, tüm vatandaşların bu eylemin önceliklerini ve kapsamını anlaması hedeflenmiştir.[56]

2013 yılında, çok sayıda Fransız işletmesinin ve kamu sektörü kuruluşunun ağ ve bilgi sistemlerine yönelik siber saldırıların sayı ve karmaşıklık açısından arttığına ilişkin değerlendirmeye yanıt olarak yeni bir Beyaz Kitap yayınlanmıştır. Yeni bir dönüm noktası olan bu Beyaz Kitapla birlikte devlet artık kendi siber güvenlik gereksinimlerini karşılamanın yanında ulusun ekonomik veya askeri potansiyelini, güvenliğini veya direncini tehdit eden faaliyetlere karşı da gerekli çalışmaları sağlayacaktır.

19 Aralık 2013 tarihinde kabul edilen Askeri Programlama Yasası da savunma ve ulusal güvenlik ile ilgili 2013 Beyaz Kitap'ında belirlenen yönergeleri izlemiştir. Bu yasama mekanizması, hayati öneme sahip ulusal kamu ve özel sektör paydaşlarının kendilerini ve ANSSI'yi bir siber saldırı durumunda daha iyi desteklemelerini sağlamıştır. Kanunun 22'nci maddesi, hayati öneme sahip kurumların güvenliğinin artırılmasına yönelik tedbirlerin alınmasını öngörmüş bu kapsamda yürütmedeki üst yöneticilere yeni yetkiler vermiştir.

16 Ekim 2015'te çıkarılan Fransız ulusal dijital güvenlik stratejisi Fransız toplumunun dijital dönüşümünü desteklemek için tasarlanmıştır. Aynı zamanda, Avrupa'nın dijital stratejik özerkliği için bir yol haritası geliştirmede Fransa'yı lider konumuna getirmeyi hedeflemiştir. ANSSI tarafından yönetilen bu strateji, dijital çağın ortaya çıkardığı sorunlara yanıt vermeye yönelik departmanlar arası koordineli çalışmaların bir sonucudur.[57]

15 Aralık 2017'de Avrupa ve Dışişleri Bakanı tarafından sunulan Fransa'nın uluslararası dijital stratejisi ise üç temel odak etrafında toplanmıştır: yönetişim, ekonomi ve güvenlik. Bu model günümüzde uygulama alanlarında gördüğümüz bölümlendirme, ağların kontrolü ve istikrarsızlaştırma eğilimlerine karşı çıkıyor. Aynı zamanda büyük Amerikan ve Çin teknoloji firmaları tarafından etkinleştirilen modellerden farklı olarak temel haklara saygı gösterilmesini, adil rekabeti ve vergilendirmeyi destekleyerek daha fazla koruma sağlamayı amaçlamaktadır.

[56] Fransa Ulusal Siber Güvenlik Ajansı https://www.ssi.gouv.fr/en/cybersecurity-in-france/cybersecurity-strategy/

[57] Fransa Ulusal Dijital Güvenlik Stratejisi https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf

2.2.4 İngiltere

İngiltere'de siber güvenlikle ilgili ilk ulusal strateji 2011'de, 2011-2015 dönemini kapsayacak şekilde yayınlanmıştır. Bu strateji belgesi ülkenin hedeflediği dört ana amaca yönelik olarak hazırlanmıştır; İngiltere'nin siber suçla mücadele ederek siber uzayda çalışmak için dünyanın en güvenli yerlerinden biri olması, siber saldırılara karşı daha dirençli olunarak ülkenin siber uzaydaki çıkarlarının daha iyi korunması, halkın güvenle kullanabileceği ve açık toplumları destekleyen açık, istikrarlı ve canlı bir siber alanın şekillenmesine yardımcı olunması ve tüm siber güvenlik hedeflerinin gerçekleşmesi için ihtiyaç duyulan ortak bilgi, beceri ve kabiliyete sahip olunması olarak ifade edilmektedir.[58] Tanımlanan hedeflere yönelik ilerlemeye ilişkin yıllık raporlar 2011'den beri yayınlanmaktadır.[59]

Kasım 2016'da yayınlanan ikinci ulusal strateji ise 2016-2021 dönemini kapsamaktadır. İngiltere'yi siber tehditlere karşı güvenli ve dirençli, 2021 yılına kadar dijital dünyada müreffeh ve kendinden emin hale getirme vizyonu ile oluşturulmuştur. Strateji özellikle her büyüklükte ve sektörden işletmenin, uygulaması kolay tavsiyeler ve araçlar sağlayarak kendilerini ve müşterilerini siber saldırıların neden olduğu zararlardan korumak için uygun adımları atmasını sağlamayı amaçlamaktadır. Daha etkili risk yönetimi için siber riskin net ticari faydalarını ve maliyetini vurgulamak için düzenleyiciler ve yatırımcılar gibi piyasa etkileyicileriyle birlikte çalışmanın gerekliliğini vurgulayarak işletmeleri harekete geçmeye ikna etmek ve farkındalık yaratmanın ötesine geçmek için profesyonel standart kurumlarıyla ortaklıklar oluşturmayı hedeflemektedir. Son olarak pazarın çözemediği siber riskleri yönetmek için doğru düzenleyici çerçevenin oluşturulması gerektiğini ifade etmekte, AB Genel Veri Koruma Yönetmeliğinin (GDPR) siber güvenlik standartlarını yükseltmek için kullanılan araçlardan biri olacağını bildirmektedir.

İngiltere sağlam, ancak dinamik bir veri yasası oluşturarak, insanlara kendi verileri üzerinde daha fazla kontrol sağlama hakkı ve kullanımı için daha fazla onay gerektirmeyi üstün tutmaktadır. Strateji ayrıca kritik altyapılara, özellikle telekomünikasyon sektörüne daha fazla vurgu yapmaktadır. Bu sektörün hedefleri öncelikle İngiltere'deki internet hizmetlerine ve

[58] İngiltere Siber Güvenlik Stratejisi, 2011 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[59] İngiltere Siber Güvenlik Stratejisi Yıllık Raporu, 2016 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

kullanıcılarına saldırmayı önemli ölçüde zorlaştırmak ve ülke üzerinde kalıcı etkiye sahip saldırı olasılığını büyük ölçüde azaltmak için endüstri ile, özellikle İletişim Servis Sağlayıcıları ile birlikte çalışmaktır. Benzer olarak diğer hedefler ise devlet sistemlerinin ve ağlarının korunmasını iyileştirmek, endüstrinin kritik ulusal altyapıların tedarik zincirinde daha fazla güvenlik oluşturmasına yardımcı olmak, yazılım ekosistemini daha güvenli hale getirerek devletin vatandaşlara sağladığı çevrimiçi hizmetler için otomatik korumalar sağlamak olarak ifade edilmektedir.

2.2.5 Japonya

Ocak 2000'de Japon hükümeti siber güvenliği bir politika alanı olarak belirleyerek ilk adımda 'Bilgi Sistemlerini Siber Saldırılara Karşı Koruma Eylem Planı'nı yayınlamıştır. 2000 yılının ortalarından sonuna kadar, siber güvenliği stratejik olarak daha ayrıntılı bir şekilde ele almak için çift yönlü bir politika yaklaşımına girişmiş olup ilk etapta hükümetin kendi içindeki BT güvenliğini sağlaması ikinci adımda da yalnızca kritik altyapı korumasını hedeflenmiştir. 10 yıl boyunca bu çift odaklı strateji, yeni kurumların oluşturulması, yeni bilgi paylaşım yolları ve yeni bilgi güvenliği stratejileri ve düzenlemeleriyle desteklenerek sürekli olarak geliştirilmiştir. 2014 yılında, Siber Güvenlikle ilgili Temel Kanunu ile Japonya'da ilk kez "siber güvenlik" terimini yasal olarak tanımlanmıştır. Yasada adı geçen siber güvenlikle, saklanan bilgilerin sızması, kaybolması veya zarar görmesi tehditlerine karşın bilgilerin güvenli bir şekilde yönetilmesi için alınması gereken önlemler bulunmaktadır.

Bu hedeflere ulaşmak için, düzenlenen temel kanun, Japon hükümeti, yerel yetkililer, kritik bilgi altyapısı sağlayıcıları, siber ile ilgili iş operatörleri ve eğitim ve araştırma kurumları için birkaç temel sorumluluk ortaya konulmaktadır.

Bakanlıklar, devlet kurum ve kuruluşları kendi siber güvenlik mevcudiyetlerinden sorumlu olmakla birlikte, Ulusal Olaylara Hazırlık ve Siber Güvenlik Stratejisi Merkezi (NISC) ile yakın işbirliği içindedirler. Bu amaçla, NISC'in iki operasyonel bileşeni vardır: Hükümet Güvenlik Operasyonu Koordinasyon Ekibi (GSOC) ve Siber Olay Mobil Yardımcı Ekibi (CYMAT). Kamu-özel işbirliği, devletin her kademesinde uygulanmaktadır. Kabine düzeyinde Bilgi Teknolojileri Stratejik Konseyi ve Siber Güvenlik Stratejik Merkezi içindeki dört komite en belirgin unsurlardır. Bakanlık düzeyinde, Savunma Bakanlığı Siber Savunma Konseyi (MOD), Ekonomi, Ticaret ve Sanayi Bakanlığı (METI) ve İçişleri ve Haberleşme Bakanlığı (MIC)

liderliğindeki Siber Saldırı Analiz Konseyi ve ayrıca Ulusal Polis Teşkilatı'nın çok sayıda Siber Terörizme Karşı Tedbir Konseyi, Japonya'nın siber güvenlik varlığını il düzeyine indirmede çok önemli roller oynamaktadır. Nisan 2019'dan bu yana en yeni üye olan Siber Güvenlik Konseyi, kamu-özel işbirliğini benzersiz ve gönüllü bir şekilde kolaylaştırmaktadır.

Tanım olarak, Japonya'da siber güvenlik, kişisel olarak tanımlanabilir bilgilerin (PII) korunmasından ayrılmamaktadır. Mayıs 2003 tarihli Kişisel Bilgilerin Korunması Yasası (APPI), Japonya'da PII'nin korunması için yasal omurgayı oluşturmaktadır. Geçtiğimiz 16 yıl boyunca önemli revizyonlardan geçen APPI, artık – AB'nin Genel Veri Koruma Yönetmeliğine (GDPR) benzer şekilde para cezalarını da kapsamaktadır. 23 Ocak 2019'da AB Komisyonu, Japonya ile ilgili yeterlilik kararını kabul ederek 'kişisel verilerin güçlü koruma garantileri temelinde iki ekonomi arasında serbestçe dolaşmasına' izin vermiştir. Bu yeterlilik kararı ile birlikte dünyanın en büyük güvenli veri akışı alanı oluşturulmuş olup Avrupalıların verileri Japonya'ya aktarıldığında yüksek gizlilik standartlarından yararlanacaktır.[60]

2.2.6 Çin

1980'li yılların sonunda Çin Halk Cumhuriyeti'nde siber güvenlik konusundaki resmi planlamalar gündeme gelmiştir. Ulusal düzeyde bilgi teknolojileri konusundaki ilk resmi girişim ise 1986 yılında "Devlet Ekonomik Bilgi Yönetimi Lider Küçük Grup" adlı yapı kurularak başlatılmıştır. 1999 ve 2001 yıllarında alınan kararlarla "Devlet Bilişim Liderlik Grubu (SILG)" kurulmuştur. Daha sonra, "Devlet Ağı ve Bilgi Güvenliği Koordinasyon Küçük Grubu (SNISCSG)", 2003 yılında SILG'nin bir alt çalışma yapısı olarak çalışmaya başlamıştır. Bu grupların temel amacı Çin'in bilgi teknolojileri alanlarında geliştirilmesi ile bilgi ve ağ teknolojilerinin kısa ve orta vadedeki rolünün Çin hükümetinin küresel rekabet kapasitesini artırmadaki önemini belirlemesi olmuştur. Bu bağlamda, bilgi ve ağ teknolojilerinde Çin'in hızlı gelişimi önemlidir.

2008 yılında teknolojik gelişmeler doğrultusunda söz konusu hedeflere ulaşmak için yürüttüğü başarılı çalışmaların ardından yeni bir yapılanmanın kurulması için SNISCSG'nin dağılmasına karar verilmiştir.

[60] Japonya Ulusal Siber Güvenlik Savunma Raporu, 2020 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf

Devletin ilan ettiği "Orta ve Uzun Vadede Bilim ve Teknolojinin Geliştirilmesi, 2006-2020 Ulusal Programı" ülkenin çağdaş teknoloji ve bilişim alanındaki gelişimi açısından kritik öneme sahiptir. Çin yerel kaynaklar aracılığıyla bilişim ve ağ teknolojilerinin geliştirilmesini temel amaç olarak belirlemiş ve bu amacın Çin halkının yaşam kalitesini ve standartlarını yükseltme amacına uygun olacağı iddiasını ortaya koymuştur. 2006 yılına kadar bilişim ve teknoloji alanlarında bu koordinasyonu sağlayamayan kurumlar arası koordinasyon bu program ile sağlanmış ve ülkenin bugünkü teknolojik seviyesine ulaşmasında önemli bir adım atılmıştır. Bu programın askeri bir amacı olmamakla birlikte bilişim sektörünün teşvik edilmesi ve enerji kaynaklarının artırılması, çevre teknolojilerinin geliştirilmesi, teşvik edilmesi amacıyla çeşitli planlar önerilmiştir.

Çin hükümetleri siber güvenlik alanında teknolojik gelişmeye, öz sermaye kullanılarak milli ve yerli yazılım-donanım üretimine ve bu üretim süreçlerinin devlet destekli kurum ve kuruluşların desteğiyle sürdürülmesine büyük önem vermiştir. Bu stratejik yaklaşımın bir sonucu olarak 2010 yılından sonra siber güvenlik alanında önemli gelişmeler sağlanmış, kritik stratejik belgeler hazırlanmış ve yeni organizasyon yapıları oluşturulmuştur. Bu bağlamda, 2012 yılında Danıştay Enformasyon Ofisi (SCIO) tarafından "Yeni Politika Görüşü (NPO)" adlı yeni bir strateji açıklanmıştır. Bu stratejinin temel amacı, Danıştay koordinasyonunda teknoloji alanında faaliyet gösteren kuruluşlar arasında bilgi paylaşımını teşvik etmek ve bilgi ve teknoloji güvenliğinin ulusal çıkarlar çerçevesinde korunmasını sağlamaktır. Bu stratejinin önceki belgelerden temel farkı ise ekonomik ve teknolojik gelişmeye izin vermenin ötesinde, devlet kurumları ve bireyler için bilgi güvenliğini sağlamak ve ağ teknolojilerinden kaynaklanan sosyal manipülasyon ve casusluk operasyonlarını önlemek gibi yeni hedeflere sahip olmasıdır. 2014 yılında "İnternet Güvenliği ve Bilişiminde Merkezi Lider Küçük Grup" adında yeni bir organizasyon kurulmuştur. Çalışma grubunun temel amacı, devlet kurumları arasında internet güvenliği ve bilişim sektörlerinin geliştirilmesi amaçları çerçevesinde gerekli koordinasyonun ve ortak siyasi inisiyatifin oluşturulması olarak belirlenmiştir. Ayrıca grubun siber güvenlik alanında hızlı ve doğru kararlar alınması ve karar verme sürecindeki zaman kaybını da azaltması öngörülmüştür.

26 Mayıs 2015 tarihinde ise Çin Savunma Bakanlığı tarafından Çin'in Askeri Stratejisi ilan edilmiştir. Bu belge ile komuta yapısını ve tüm askeri unsurlarının ağ teknolojisi ile senkronize edilmesi zorunluluğuna vurgu yapılmıştır. Siber güvenlik alanındaki yeni girişimlere bağlı olarak uzay teknolojilerinden kaynaklanan bilimsel gelişmeleri askeri kapasitesini geliştirmek

için yeni bir fırsat alanı olarak gören Çin hükümeti, uzay teknolojileri alanında siber kapasitesini geliştirme yönünde adımlar atmıştır. Bu çerçevede, Çin Siber Uzay İdaresi tarafından 27 Aralık 2016 tarihinde yayınlanan 'Ulusal Siber Güvenlik Stratejisi' adlı belgede, siber uzayın ülke güvenliği için yeni tehdit oluşturabilecek bir alan olduğu, bu alandan kaynaklanacak her tür tehdidin bertaraf edilmesi için hükümet tarafından bilimsel, teknik, hukuki, diplomatik ve askeri tedbirlerin alınacağı ifade edilmektedir. Stratejiye göre açık piyasa, şeffaflık ve rekabet koşullarına sahip bir ekonomi modeli desteklenecek ve bilişim ve teknoloji sektörlerinde yerel şirketlerin uluslararası yatırımlarını artırmaları teşvik edilecektir. Uzay teknolojilerine ilişkin siber kapasitenin geliştirilmesinde bir diğer kritik referans noktası, 1 Mart 2017'de Çin Dışişleri Bakanlığı ve Çin Siber Uzay İdaresi tarafından yayınlanan "Siber Uzayda Uluslararası İşbirliği Stratejisi"dir. Kısaca özetlemek gerekirse, bu belgede siber uzayın askerileştirilmesine ve caydırıcılık alanı olarak kullanılmasına karşı çıkıldığı, uluslararası güvenlik ve istikrara yönelik bu tür girişimlerin siber uzay tarafından denetlenmesi ve kontrol edilmesi gerektiği hususları yer almıştır. Bu noktada devletlerin, uluslararası kuruluşların, uluslararası şirketlerin, sivil toplum kuruluşlarının ve hatta bireylerin dahil olduğu çok taraflı bir yönetişim olan Birleşmiş Milletler'in (BM) söz konusu denetim komitelerinin belirlenmesi için uygun bir zemin olduğu ifade edilmektedir.[61]

3 TÜRKİYE İNCELEMESİ

Siber suçlar, bir başka deyişle bilişim suçları, mücadele edilmesi bakımından diğer suçlara nazaran ayrı bir yere sahiptir. Çünkü siber suç kavramı oldukça yeni bir olgudur ve suçun işlenişine yönelik şablonlar çıkarmak bir hayli zor olmaktadır. Sürekli gelişen ve değişen siber mecrada yaşanan hak ihlalleri ve suçlara yönelik yaptırımlar ortaya koymak, bu hareketlilik içerisinde yaptırımlarda süreklilik ve değişimlere uyum sağlamak gerekmektedir. Tüm bunların yanı sıra suçların tanımlanması zordur ve fail ile mağdur arasında zaman-mekân açısından mesafeler bulunmaktadır. Yani fiziki hayatta işlenen suçlarla karşılaştırıldığında siber suçlar çok daha farklı bir uzayda gerçekleşmekte ve buna bağlı olarak farklı kurallara ve cezalara tabi olmaktadır.[62]

[61] NURKULOV Nurshod, New Cyber Strategy Of China And The Alterations İn The Field, University of World Economy and Diplomacy, Özbekistan, Ocak 2017 https://www.researchgate.net/publication/322739786_New_Cyber_Strategy_of_China_and_the_Alterations_in_the_Field

[62] ÖNOK Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş birliği," Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 19, Sayı: 2 (Aralık, 2013): 1232-1235. https://dergipark.org.tr/tr/download/article-file/814473

Teknik olarak açıklamak gerekirse siber suç politika veya stratejilerinin temel unsurları; önleyici tedbirlerin alınması, mevzuatın oluşturulması, siber suçlarla mücadelede özel kolluk birimleri ve özel savcılık hizmetlerinin oluşturulması, kurumlar arası iş birliğinin sağlanması, kolluk ve adli personel eğitimi, kamu/özel sektör işbirliği, etkili uluslararası işbirliği, kara para aklamanın ve dolandırıcılığın önlenmesi için mali soruşturma ve cinsel şiddete karşı çocukların korunması olarak kabul edilmektedir. Bu unsurlar, siber suçlarla mücadele politikasının belirlenmesi ve uygulanmasında, birden fazla aktörün birbirleriyle bağlantılı bir biçimde rol oynadığını ortaya koymaktadır.[63]

3.1 Hukuki Boyut ve Dijital Suçlarla İlgili Yapılan Düzenlemeler

20. yüzyılın ortalarından itibaren kullanılmaya ve gelişmeye başlayan bilgi ve iletişim teknolojileri her geçen gün hayatın tüm alanlarında büyük değişikliklere sebep olmakta, bu teknolojilerin ortaya çıkardığı yeni araçlar ve hizmetler hızla insanlığın tüm yaşamını etkilemeye devam etmektedir. Bilişim teknolojileri ve sunduğu hizmetler nitelikleri gereği sadece ulusların milli düzenlerini değil tüm uluslararası toplumu etkilemekte, bu nedenle modern dünyadaki ülkeler ve uluslararası örgütler bu alanda işbirliğine giderek baş döndürücü bir hızda gelişen bu yeni ortama ayak uydurmaya çalışmaktadır. Artık herkesin benimsediği gibi, bilgi teknolojileri ürünleri ve bilgi toplumu hizmetleri modern bireyin günlük hayatını neredeyse çepeçevre kuşatmış bulunmaktadır. Başta bilgisayarlar olmak üzere internete bağlanabilen cep telefonları, bankamatikler, internet üzerinden gerçekleştirilebilen bankacılık işlemleri ve çeşitli kamu hizmetlerinin bilişim ağları üzerinden verilebilmesi, modern hayatta insanlığın yaşamını kolaylaştırmak için çok büyük imkânlar sunmaktadır. Bilişim teknolojilerinin çok hızlı değişmesi ve şekillenmesi ile sınır tanımaz niteliği bu alanda düzenleme yapılmasını da gerekli hale getirmektedir. Bilişim ortamında işlenen suçların hızlı bir şekilde artışı, bu suçların ortaya çıkarılmasındaki zorluklar ve işlenmesindeki kolaylıklar ve ekonomik olarak meydana gelen zararın büyüklüğü bu konuda yasal bir düzenleme yapılmasının zorluğunu açıkça ortaya koymaktadır.[64]

Dünyada bilişim suçlarıyla ilgili düzenlemelerde iki ayrı metodun kullanıldığı görülmektedir. ABD, İngiltere, İrlanda ve Portekiz gibi ülkelerin dahil olduğu birinci sistemde mevcut

[63] TAŞCI Ufuk ve CAN Ali, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014," Fırat Üniversitesi Sosyal Bilimler Dergisi 25, Sayı 2 (Temmuz, 2015): 232. https://dergipark.org.tr/tr/download/article-file/157433

[64] https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/

kanunlardan ayrı olarak yeni ve özel düzenlemeler oluşturulmaktadır. Alman mevzuatının öncülük ettiği ikinci sistemde, suç teşkil eden eylemler mevcut kanunlar dahilinde incelenmekte, ayrı fasıllar ve kanunlar oluşturulmamaktadır. Bu sistemde suç tarifleri bilişim suçlarını kapsayacak şekilde değiştirilerek veya kanunlara yeni fiiller eklenerek karşılaşılan sorunlar çözülmeye çalışılmaktadır.[65]

Dünyada yaşanan süratli gelişmelere paralel olarak ülkemizde bilgisayar, hayatın her aşamasında pozitif ve negatif yönüyle etkin bir şekilde kullanılmaktadır. Ülkemizde bilgisayar ve internet kullanımı 2020 yılında 16-74 yaş grubundaki bireylerde sırasıyla %79,0 ve %90,7 iken 2021 yılında sırasıyla %82,6 ve %92,0 olmuştur. Bilgisayar ve internet kullanımının tüm dünya ile paralel olarak ülkemizde de artmasıyla birlikte, ülkemizde de bu alanda ortaya çıkan suçlara ilişkin önlemler ve yasal düzenlemeler yapma ihtiyacı hâsıl olmuştur.[66]

Ülkemiz bilişim suçlarıyla mücadele alanında dünyada önemli bir konuma sahiptir. Gerek 2021 yılı şubat ayı itibariyle 83,6 milyona ulaşan nüfusuyla gerekse de nüfusun internet kullanım oranıyla bu alanda öne çıkan ülkelerden birisidir. Türkiye'de birçok üniversitede bilişim ve teknoloji alanında önemli gelişmeler takip edilmekte ve özellikle son dönemde dünya çapında popüler olan yeni teknoloji trendlerinde önemli çalışmalar yapılmaktadır. Bu kapsamda teknolojiyi ve interneti iyi kullanan bir ülke olarak, ülkemizde de bu alanda işlenen suçlarda artış gözlemlenmektedir. Yurtiçine ve yurtdışına yönelik siber saldırılar ülkemiz üzerinden veya ülkemize yönelik olarak yapılabilmektedir.

Türkiye ise gerek Anayasası'ndaki bireylerin haklarını taahhüt altına alan yükümlülükleri ile Avrupa Konseyi'nin Siber Suçlar Sözleşmesi'ndeki yükümlülüklerini yerine getirmek gerekse bu alanda işlenen suçlarla etkin mücadele edebilmek amacıyla hem 5237 sayılı TCK'da bu alandaki suçları ayrı bir başlık altında toplayarak detaylandırmış hem de çeşitli hukuki düzenlemeler yapma yoluna gitmiştir. Bu hukuki düzenlemeler detaylı şekilde ilerleyen kısımlarda ele alınacaktır.

[65] https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/
[66] TÜİK, Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması 2021, 26 Ağustos 2021 https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437

3.1.1 Türkiye Cumhuriyeti Anayasası

1982 yılında kabul edilen, 1987, 2010 ve 2017 yıllarında değişiklikler yapılan Türkiye Cumhuriyeti Anayasasının "**Kişinin Hakları ve Ödevleri"** başlıklı ikinci bölümünde;

a) Özel Hayatın Gizliliği ve Korunması (Madde 20)

"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

b) Haberleşme Hürriyeti (Madde 22)

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz." ifadeleriyle özel hayatın gizliliği ve haberleşme hakkı devlet güvencesi altına alınmış ve değişik kanunlarda konuyla ilgili düzenlemeler yapılmıştır.

3.1.2 5237 Sayılı Türk Ceza Kanunu

01.06.2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nda bilişim yoluyla işlenen suçlar değişik başlıklar halinde ve çok kapsamlı olarak ele alınmış, kişilerin korunması ve suçların önlenebilmesi amacıyla suçlulara ağır müeyyideler getirilmiştir.

Kanunun "Topluma Karşı Suçlar" başlıklı Üçüncü Kısmının Onuncu Bölümü "Bilişim Alanında Suçlar" başlığını taşımaktadır. Bu başlığın alt maddelerinde bilişim alanındaki suçlar değişik şekillerde açıklanmış, bu suçların işlenmesi halinde cezai müeyyideler konulmuş ve aşağıdaki ifadelere yer verilmiştir.

Bilişim sistemine girme

Madde 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(4) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 244- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Kanunun, "Kişilere Karşı Suçlar" başlıklı İkinci Kısmının "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı Dokuzuncu Bölümünde de bilişim yoluyla işlenebilecek olan suçlara ilişkin olarak aşağıdaki ifadelere yer verilmiştir.

Haberleşmenin gizliliğini ihlal

Madde 132- (1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması

Madde 133- (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(3) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

Madde 134- (1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

Kişisel verilerin kaydedilmesi

Madde 135- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

Verileri hukuka aykırı olarak verme veya ele geçirme

Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Yine Kanunun, "Kişilere Karşı Suçlar" başlıklı İkinci Kısmının "Mal Varlığına Karşı Suçlar" başlıklı Onuncu Bölümünde "Nitelikli Hırsızlık" ve "Nitelikli Dolandırıcılık" fiilleri tanımlanmış ve bu suçlara ilişkin aşağıdaki ifadelere yer verilmiştir.

Nitelikli Hırsızlık

Madde 142-

(2) Suçun;

e) Bilişim sistemlerinin kullanılması suretiyle, işlenmesi hâlinde, beş yıldan on yıla kadar hapis cezasına hükmolunur.

Nitelikli dolandırıcılık

Madde 158- (1) Dolandırıcılık suçunun;

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle, işlenmesi halinde, üç yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur. Ancak, (e), (f), (j), (k) ve (l) bentlerinde sayılan hâllerde hapis cezasının alt sınırı dört yıldan, adli para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz.

Yine Türk Ceza Kanunu'nun Topluma Karşı Suçlar başlıklı Üçüncü Kısmının Yedinci Bölümü "Genel Ahlaka Karşı Suçlar" başlığını taşımaktadır. Bu başlığın alt maddelerinde de bilişim alanındaki suçlar açıklanmış ve bu suçların işlenmesi halinde uygulanacak cezai müeyyideler aşağıdaki şekilde açıklanmıştır.

Kumar oynanması için yer ve imkân sağlama

Madde 228-

(3) Suçun bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde üç yıldan beş yıla kadar hapis ve bin günden onbin güne kadar adlî para cezasına hükmolunur.

Bilişim suçları ile mücadelede ceza hukukunun ve yargılamasının beraber ele alınmasıyla netice elde edilmesi mümkün olacaktır. Bilişim suçlarının milletlerarası kalitede olması nedeniyle kabahatin işlenmesi ve failin yargılanması açısından taraf olunan Avrupa Siber Suçlar Sözleşmesi önem kazanmaktadır. Sözleşmenin "Uluslararası İşbirliğiyle Alakalı Genel Prensipler" isimli 23. maddesinde "Taraf devletlerden bilgisayar sistem ve verileri hakkında işlenen suçlarda ve herhangi bir suçun elektronik ortamda bulunan delilinin elde edilmesinde gerek Sözleşme'nin uluslararası işbirliğine ilişkin bölümünde yer alan hükümlere gerek cezai alanda uluslararası işbirliği ile ilgili tek taraflı veya çoklu antlaşmalara göre mümkün olan en geniş biçimde birbirleri ile işbirliği yapmaları gerektiği" hükmü yer almaktadır. Düzenleme gereği, uluslararası işbirliğinin sağlanabilmesi için işbirliğine gidecek devletlerin mevzuatlarının birbirleriyle uyumlu olması ve teknik altyapılarının yeterli olması gerekmektedir.

3.1.3 5070 Sayılı Elektronik İmza Kanunu

23.01.2004 tarihli 5070 sayılı Elektronik İmza Kanununda elektronik imzanın hukukî yapısı, elektronik sertifika hizmet sağlayıcılarının faaliyetleri ve her alanda elektronik imzanın kullanımına ilişkin işlemler ele alınmaktadır.

Elektronik İmza Kanunu'nun 3. maddesinde elektronik imza, "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" ve imza sahibi kişi ise "Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi" olarak tanımlanmıştır.

Elektronik İmza Kanunu'nun 8. maddesinde ise Elektronik sertifika hizmet sağlayıcısının tanımı "Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri" şeklinde yapılmıştır.

Elektronik İmza Kanunu'nun "Bilgilerin korunması" başlıklı 12. maddesinde elektronik sertifika hizmet sağlayıcısının yükümlülükleri aşağıdaki şekilde açıklanmıştır. Elektronik sertifika hizmet sağlayıcısı;

a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,
b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,
c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

Elektronik İmza Kanunu'nun 16. ve 17. maddelerinde adli suçlar, 18 ve 19. maddelerinde ise idari suçlar düzenlenmiştir. 16. ve 17. Maddelerde bilişim suçu kapsamına giren ilgili kişinin rızası dışında elektronik imza oluşturma ve sahtekarlık suçlarına karşı uygulanacak hukuki müeyyideler tanımlanmıştır. Bu maddelerde suç tanımları ve uygulanacak adli cezalar aşağıdaki şekilde açıklanmaktadır.

İmza oluşturma verilerinin izinsiz kullanımı

Madde 16- Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Elektronik sertifikalarda sahtekârlık

Madde 17- Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

İdarî para cezaları

Madde 18- Bu Kanunun;

a) 10 uncu maddesindeki yükümlülüklerinden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına onbeşbin Türk Lirasından otuzbin Türk Lirasına kadar,
b) 11 inci maddesindeki yükümlülüklerden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına onikibin Türk Lirasından yirmibin Türk Lirasına kadar,
c) 12 nci maddesi hükümlerine aykırı hareket edenler hakkında onbeşbin Türk Lirasından otuzbin Türk Lirasına kadar,
d) 13 üncü maddesinin beşinci ve yedinci fıkralarındaki yükümlülükleri yerine getirmeyen elektronik sertifika hizmet sağlayıcısına onikibin Türk Lirasından yirmibin Türk Lirasına kadar,
e) 15 inci maddesi hükümlerine aykırı hareket eden elektronik sertifika hizmet sağlayıcısına otuzbin Türk Lirasından ellibin Türk Lirasına kadar,

idarî para cezası Bilgi Teknolojileri ve İletişim Kurumu tarafından verilir. Bu madde hükümlerine göre ilgili tüzel kişi hakkında verilecek olan idarî para cezasının üst sınırı yetmişbeşbin Türk Lirasıdır.

Tüzel kişilere özgü güvenlik tedbirleri

Madde 19- Bu Kanunda tanımlanan suçlar dolayısıyla ilgili tüzel kişiler hakkında Türk Ceza Kanununun 60 ıncı maddesi hükmüne göre tüzel kişilere özgü güvenlik tedbirlerine hükmolunur.

İdarî para cezasını gerektiren eylemlerin işlendikleri tarihten itibaren geriye doğru üç yıl içinde üçüncü kez işlenmesi hâlinde Kurum tarafından elektronik sertifika hizmet sağlayıcısı tüzel kişinin faaliyet izninin iptaline karar verilir.

3.1.4 5809 Sayılı Elektronik Haberleşme Kanunu

10.10.2008 tarih ve 5809 sayılı Elektronik Haberleşme Kanununun 4. maddesinde İlkeler başlığı altında "İlgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde bilgi güvenliğini ve haberleşme gizliliğini gözetme" ilkesine yer verilmektedir.

Ayrıca Elektronik Haberleşme Kanununun "Kurumun görev ve yetkileri" başlıklı 6. Maddesinde siber suçlara ilişkin aşağıdaki hükümlere yer verilmektedir.

MADDE 6 - (1) Kurumun görev ve yetkileri şunlardır:

c) Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.

h) İşletmecilerin ticari sırları ile kamuoyuna açıklanabilecek bilgilerinin kapsamını belirlemek, işletmecilerin ticari sırları ile yatırım ve iş planlarının gizliliğini korumak ve bunları adli makamların talepleri dışında muhafaza etmek.

v) Siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek.

Yine Kanunun "İşletmecilerin hak ve yükümlülükleri" başlıklı 12. Maddesinde işletmecilere kişisel veri ve gizliliğin korunması yükümlülüğü getirilmiştir.

Ayrıca Elektronik Haberleşme Kanununun "Tüketici ve Son Kullanıcı Hakları" başlıklı Dördüncü Kısmında "Kişisel verilerin işlenmesi ve gizliliğin korunması" başlığı ile aşağıdaki hükümler konulmuştur.

MADDE 51 –

(1) Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.

(2) Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaktır.

(3) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.

(4) İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır.

(5) Bu Kanunun 49 uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel veriler işlenebilir.

(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verileri ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabilir.

(7) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak

saklanır. Katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla ihtiyaç duyulan trafik verileri ile konum verileri anonim hâle getirilerek veya ilgili abonelerin/kullanıcıların açık rızalarının alınması ve sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla, belirtilen faaliyetlerin gerektirdiği ölçü ve sürede işlenebilir.

(8) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

(9) Abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel veriler, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebilir.

(10) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince,

saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir.

(11) Tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine ve elektronik kimlik bilgisini haiz cihazlara yönelik tarafların kendi sistemlerinde oluşan fatura tutarı ve ödeme bilgileri ile sahtecilik, dolandırıcılık riski içeren şüpheli veya zarar doğurucu vakalara ve işlem hareketlerine ilişkin kayıtlar, işletmeciler ve Kurumun MCKS'si arasında paylaşılabilir veya işlenebilir.

(12) Bu Kanun kapsamında kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmeciler sorumludur.

(13) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

3.1.5 5651 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"

İnternette yer alan yasa dışı içeriklerle mücadele amacıyla 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 23/5/2007 tarihinde Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

Bu kanun kapsamında internet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesi/içeriğin çıkarılması kararı verilebileceği düzenlenmiştir.

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;
1) İntihara yönlendirme (madde 84),
2) Çocukların cinsel istismarı (madde 103,birinci fıkra),
3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
4) Sağlık için tehlikeli madde temini (madde 194),
5) Müstehcenlik (madde 226),
6) Fuhuş (madde 227),
7) Kumar oynanması için yer ve imkân sağlama (madde 228),

suçları.

b) 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar,

c) 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar.

3.1.6 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Bilişim alanındaki hukuksal düzenlemelerin ilgilendiği temel sorun alanlarından bir diğeri; kişisel verilerin korunmasıdır. Teknolojinin ilerlemesi ve mahremiyet artırıcı teknolojilerin ortaya çıkması ile kişisel mahrem ve gizli bilgilerin korunması zorlaşmıştır.

Kişisel veri; bilinen veya kimliği tespit edilebilir gerçek ve tüzel kişilere ilişkin tüm bilgilerdir. Veri, her türlü bilgiyi kapsarken; kişisel veriler sadece bireylerin kimliklerine doğrudan veya dolaylı olarak ulaşılmasına olanak veren bilgileri içermektedir. Kişisel verilerin ihlali ise,

kişinin özgür iradesiyle verdiği kabul beyanı dışında, yetkisi olmadığı halde ya da hukuka aykırı olarak kişisel verilerin zarara uğramasına, kaybolmasına, iletilmesine, değiştirilmesine, herhangi bir yere depolanmasına, kaydedilmesine, işlenmesine, açığa çıkarılmasına ve ilgili verilere erişilmesine neden olan güvenlik ihlalidir.[67]

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla 7 Nisan 2016 tarihinde 6698 sayılı kanun yayımlanmıştır. Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanmaktadır. Bu Kanunla verilen görevleri yerine getirmek üzere, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu (KVKK) kurulmuştur.

Kişisel Verilerin Korunması Kanununun "**Suçlar ve Kabahatler**" başlıklı 5. Bölümünde aşağıdaki hükümlere yer verilmektedir.

Suçlar

MADDE 17- (1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.

(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.

Kabahatler

MADDE 18- (1) Bu Kanunun;

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,

b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,

c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,

[67] GÖNEN Serkan, ULUS Halil İbrahim, YILMAZ Ercan Nurcan, ResearchGate, Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, Bilişim Teknolojileri Dergisi, Cilt: 9, Sayı: 3, Eylül 2016 https://www.researchgate.net/publication/308821569_Bilisim_Alaninda_Islenen_Suclar_Ve_Kisisel_Verilerin_Korunmasi/link/5b6c557d299bf14c6d97b303/download, s. 233

ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar,
idari para cezası verilir.

(2) Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

(3) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.

3.1.7 Siber Güvenlik Stratejisi ve Eylem Planı

Ülkemizde siber güvenlik alanında ilk olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 20 Haziran 2013 tarihli ve 28683 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. 2 yıllık bu dönem içerisinde siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik farkındalığının oluşturulması, siber tehditlerin tespiti ve önlenmesi konularında çalışmalar yürütülmüştür. Ayrıca 2013 yılında, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş, belirlenen kritik altyapı sektörleri başta olmak üzere kurum ve kuruluşlarda Siber Olaylara Müdahale Ekipleri (SOME) faaliyetlerine başlamıştır. Ulusal siber güvenlik organizasyonunun oluşturulmasıyla ülkemizde kurumsal ve organizasyonel yapıların kurularak güçlendirilmesi sağlanmıştır.

Sonrasında yayımlanan "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile de siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulabilmesi için siber savunmanın güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele edilmesi, farkındalık ve insan kaynağı geliştirilmesi, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu konularında çalışmalar yürütülmüştür. Bu çerçevede, son dönemde;

- Ulusal siber güvenlik kapasite inşası programı kapsamında SOME'lerin insan kaynağının iyileştirilmesi ve siber olaylara hazırlık seviyesinin artırılması, ülkemizin ihtiyaç duyduğu insan kaynağının yetiştirilmesine yönelik olarak eğitim, kamp ve yarışma gibi faaliyetler,

- Teknolojik önlemler programı kapsamında, yapay zekâ ve makine öğrenmesi imkânlarını kullanan AVCI, AZAD, KASIRGA gibi hızlı tespit ve erken müdahale sistemlerinin geliştirilmesi,
- Tehdit istihbaratı edinimi, üretimi ve paylaşımı programı kapsamında ulusal ve uluslararası paydaşlarla iki yönlü bilgi paylaşımı ve koordinasyon çalışmaları ve
- Kritik altyapıların korunması programı kapsamında kritik altyapıların hizmet sürekliliğinin takibine yönelik izleme faaliyetleri, zafiyet tarama çalışmaları ve bilgi güvenliği açısından düzenleme ve denetleme çalışmaları yürütülmüştür.

Teknolojinin vazgeçilmezliği ve sürekli gelişimiyle birlikte siber güvenliğe ilişkin faaliyetlerin de süreklilik içerisinde yürütülmesi gerekmektedir. Bu doğrultuda, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), bugüne kadar gerçekleştirilen çalışmalarda elde edilen kazanımların daha ileriye taşınması amacıyla hazırlanmış ve 29 Aralık 2020 tarihinde Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Siber tehditlerin etkilerinin azaltılması, ulusal kabiliyetlerin geliştirilmesi, daha güvenli bir ulusal siber ortamın oluşturulması ve ülkemizin siber güvenlik alanında uluslararası seviyede en üst sıralarda yer alması hedeflenmektedir. Hazırlanan strateji ve eylem planında yer alan 8 stratejik amaç, 40 adet eylem ve 75 adet uygulama adımı ile ülkemizin 2023, 2053 ve 2071 hedefleri doğrultusunda ilerleme sağlanmaktadır.

Ulusal Siber Güvenlik Stratejisi ve 2020-2023 Eylem Planının hedefleri şunlardır;

1) Kritik altyapılarımızın siber güvenliğinin 7/24 korunması,
2) Ulusal seviyede siber güvenlik alanında en son teknolojik imkânlara sahip olunması,
3) Operasyonel ihtiyaçlar çerçevesinde yerli ve milli teknolojik imkânların geliştirilmesi,
4) Siber olaylara müdahalenin olay öncesi, esnası ve sonrasını kapsayan bir bütün olmasından hareketle; proaktif siber savunma anlayışının geliştirilmeye devam edilmesi,
5) Siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin ölçülmesi ve izlenmesi,
6) Siber olaylara müdahale ekiplerinin yetkinliklerinin artırılması,
7) Kurumsal, sektörel ve ulusal bazda siber olaylara hazırlık seviyelerinin risk temelli analizler ve planlamalara dayalı yaklaşımlarla artırılması,
8) Kurum ve kuruluşlar arası veri paylaşımının güvenli biçimde sağlanması,
9) Kaynağı ve hedefi yurt içi olan veri trafiğinin yurt içinde kalması,
10) Kritik altyapı sektörlerinde düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi,

11) Kritik altyapı sektörlerinde, BT ürünlerinde üretici bağımlılığının önüne geçilmesi,
12) Yeni nesil teknolojilerin güvenliğinin sağlanmasına yönelik gereksinimlerin belirlenmesi,
13) Yenilikçi fikirlerin ve Ar-Ge faaliyetlerinin desteklenerek yerli ve milli ürün ve hizmetlere dönüşümünün gerçekleştirilmesi,
14) Toplumun tüm kesimleri tarafından siber uzayın güvenle kullanılması,
15) Siber güvenlik farkındalığının tüm toplumda üst seviyede tutulmasına yönelik etkinliklerin sürdürülmesi,
16) Kurum ve kuruluşlarda kurumsal bilgi güvenliği kültürünün yerleşmesi,
17) Çocukların siber ortamda korunmasının sağlanması,
18) Siber güvenliğe ilgi duyan veya uzmanlaşmak isteyen bireylere yönelik projelerle insan kaynağının güçlendirilmesi,
19) Örgün ve yaygın eğitimde siber güvenlik eğitiminin yaygınlaştırılması ve eğitim içeriklerinin zenginleştirilmesi,
20) Ulusal ve uluslararası düzeydeki paydaşlarla bilgi paylaşımı ve iş birliğini sağlayacak mekanizmaların geliştirilmesi. Siber suçların en aza indirgenmesi ve caydırıcılığın artırılması ve
21) İnternet ve sosyal medyada doğru ve güncel bilgi paylaşımının sağlanmasına yönelik mekanizmaların geliştirilmesidir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında belirlenen hedefler ve eylemlerin ilgili kurum ve kuruluşlarca hayata geçirilmesi, tüm paydaşların etkin iletişimi ve iş birliği içerisinde faaliyetlerini yürütmesi ülkemizin siber güvenliğine büyük katkı sağlayacağı değerlendirilmektedir.

3.2 Polisiye Yöntemler

Siber suçlarla mücadelede polisiye yöntemler İçişleri Bakanlığı'na bağlı Emniyet Genel Müdürlüğü üzerinden yürütülmektedir. EGM'nin Bilişim Suçlarını gündemine alması 2003 yılına kadar gitmektedir. Öncelikle Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı bünyesinde Bilişim Suçları ve Sistemleri Şube Müdürlüğü kurulmuş, daha sonra bu şube müdürlüğü ise 15 bölge merkezinde Adli Bilişim Büro Amirlikleri kurmuş ve Adli Bilişim Uzmanları yetiştirmiştir. Daha sonra yine adı geçen şube müdürlüğü tarafından 80 ilde Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlükleri ve bunların bünyesinde de Bilişim Suçları Büro Amirlikleri kurulmuştur. 2010 yılını müteakip Bilişim Suçları ve

Sistemleri Şube Müdürlüğü ikiye bölünerek Bilişim Suçları Şube Müdürlüğü tek başına ayrı bir müdürlük olarak işlemeye başlamış, 2014'ten sonra ise siber suçlar gündemi ve ilgili teşkilatların çalışmaları ivme kazanmıştır. Siber Suçlar Daire Başkanlığı tek başına bir bünye olarak yolunda devam etse de Güvenlik, Asayiş, KOM ve Terör Daire Başkanlığı gibi birimlerle iş birliği içinde çalışılmış, bir süre sonra bu yapılara bazı Türk hacker'lar da dâhil olmuştur.[68]

Söz konusu şube müdürlüğünün görevleri şöyle sıralanabilir:

- 5237 sayılı Kanunun 243'üncü ve 244'üncü maddelerinde belirtilen suçlarla mücadele etmek ve bu kanunlarda belirtilen diğer suçların işlenmesi durumunda gerekli çalışmayı yapmak veya gerektiğinde ilgili kurum ve kuruluşlara teknik destek vermek,
- Bilişim sistemleri yoluyla işlenen 5237 sayılı Kanunun 245 inci maddesinin birinci, ikinci ve üçüncü fıkrasında yer alan görev alanına giren suçlarla mücadele etmek,
- 5070 sayılı Elektronik İmza Kanunu'nun 16 ve 17'nci maddelerini kapsayan suçlarla mücadele etmek,
- 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 23'üncü maddesi kapsamındaki suçlarla mücadele etmek,
- Görev alanına giren konularda İl KOM Birimleri tarafından yürütülen mücadeleyi yönlendirmek, çalışmalarla ilgili eksikliklerin giderilmesi için girişimlerde bulunmak,
- Görev alanına giren konularda, Başkanlıkça belirlenen kriterler, ikili ve uluslararası anlaşmalar ile ulusal mevzuat çerçevesinde yabancı ülke makamlarından veya irtibat görevlilerinden gelen talepleri değerlendirmek ve gerekli işlemleri yürütmek,
- Görev alanına giren konularda mevzuat çerçevesinde ulusal veya uluslararası kuruluş faaliyetlerine katılmak ve sonucunda Başkanlığa rapor sunmak,
- Görev alanına giren konularda idari ve hukuki eksikliklerin giderilmesi ve geliştirilmesi yönünde görüş ve önerilerde bulunmak,
- Başkanlık ve İl KOM Birimlerinde karşılaşılan bilişim sistemleriyle ilgili her türlü problemleri çözüme kavuşturabilmek için gerekli alt yapı ve tespit edilen projelerle ilgili analiz çalışmaları yapmak ve uygun çözümleri ortaya koymak ve
- Bilişim Suçları veya diğer operasyonel birimlerine Adli Bilişim hizmeti vermektir.[69]

---

[68] TAŞCI Ufuk ve CAN Ali, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014," Fırat Üniversitesi Sosyal Bilimler Dergisi 25, Sayı 2, Temmuz 2015 https://dergipark.org.tr/tr/download/article-file/157433

[69] ÖZÜDOĞRU Uğur, Siber Suçlar ve Mücadele Yöntemleri Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri, BTK Bilişim Uzmanlığı Tezi, 2011: 121-122. https://docplayer.biz.tr/57366564-Siber-suclar-ve-mucadele-vontemleriz-dunya-uygulamalari-ve-turkiye-icin-cozum-onerileri.html

3.3 Teknik Yöntemler

Siber suçlarla mücadele kapsamında kullanılan teknik yöntemler; siber güvenlik ve adli bilişim süreçleri olarak ikiye ayrılmaktadır. Siber güvenlik temel olarak siber uzayın her açıdan korunması anlamına gelir ve bütüncül/derleyici bir kavramdır. Bu kavram en küçük suçlardan oldukça karmaşık büyük saldırılara kadar, siber güvenliği tehdit eden her türlü unsuru içerisine alır. Siber güvenlik olgusu verinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması kavramlarının çatısı olarak kabul edilebilir. Hatalar, kazalar ve saldırılardan oluşan siber tehditlere karşı siber suçlar ve bunlarla mücadele, askeri siber organizasyon ve operasyonlar, istihbarat ve karşı istihbarat, kritik altyapı koruması ve ulusal kriz yönetimi, siber diplomasi ve internet yönetişimi başlıkları ulusal siber güvenliğin tabanını oluşturur.[70]

Adli bilişim süreçleri gerçek hayatta işlenmiş bir suçu aydınlatmak adına olay yerinden delil toplanması gibi suçun işlendiği siber uzay ortamından daha teknik bir yöntemle deliller toplanmasıdır. Bu çalışmalara kaybolan verilerin tekrar ortaya çıkarılması, veri analizleri, geriye dönük kayıt incelemeleri gibi süreçler örnek verilebilir.[71]

3.3.1 Siber Güvenlik

Siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür. Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır.

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefleri erişilebilirlik, bütünlük

[70] BIÇAKÇI Salih, Siber Güvenlik ve Savunma, Güvenlik Yazıları, Sayı: 42 (Kasım, 2019): 2-3. https://www.researchgate.net/publication/337569798_Siber_Guvenlik_ve_Savunma

[71] DÜLGER Murat Volkan, Adli Bilişim & Ülkemizde Uygulanması, İstanbul Aydın Üniversitesi, Mayıs 2017, https://www.researchgate.net/publication/318792740_Adli_Bilisim_ve_Ulkemizde_Uygulamasi

(aslına uygunluk ve inkâr edilemezliği de kapsar) ve gizliliktir (ITU – T X.1205 sayılı Tavsiye Kararında yer alan ve uluslararası alanda kabul gören tanımdır).[72]

Siber güvenlik üzerine yapılan çalışmaları iki ana kategoride değerlendirebiliriz. Bunların birincisi devlet ve kurumları tarafından alınan önlemler ve diğeri de kişisel önlemler olarak sıralanabilir.

Siber Güvenlik Kurulu: Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu karar gereğince Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır.

Bilgi Teknolojileri ve İletişim Kurumu (BTK): Devlet eliyle tedbir alan kurumların başında 2000 yılında Telekomünikasyon Kurumu olarak kurulan, 2008'de Bilgi Teknolojileri ve İletişim Kurumu olarak adı değiştirilen yetkili kurum gelmektedir. Kurum telekomünikasyon araçları vasıtasıyla yapılan iletişimin ve sinyal bilgisinin takibi, gözetlenmesi, değerlendirilmesi ve kaydedilmesi, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcılarının denetlenmesi, yine aynı zamanda içerik, erişim ve yer sağlayıcıları ile diğer kurumların siber saldırıları tespit etmesi ve engellemesi görevlerini yürütmektedir.

06/02/2014 tarihinde yayımlanan 6518 saylı kanun ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na bazı maddeler eklenerek ilgili Bakanlar Kurulu kararı güncellenmiş, Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili aşağıdaki görevler verilmiştir:

- Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi (4 üncü madde birinci fıkra (ı) bendi),
- İzinsiz erişime karşı şebeke güvenliğinin sağlanması(12 nci madde ikinci fıkra (j) bendi),
- Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması (6 ncı madde birinci fıkra (ş) bendi),

[72] https://www.btk.gov.tr/siber-guvenlik-genel-bilgi

- Siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek (6 ncı madde birinci fıkra (v) bendi).

Diğer taraftan, "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" kapsamında, Ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel siber saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 27/05/2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur. Ayrıca 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulmuştur. USOM ve SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları öncelemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde hayati önemi olan yapılardır. USOM ile Kurumsal SOME ve/veya Sektörel SOME'nin koordineli çalışması ve işbirliği halinde olması ulusal siber güvenliğimize katkı sağlamaktadır. Siber güvenlik olaylarına maruz kalan bilişim sistemlerine yönelik koruyucu tedbirlerin alınması konusunda faaliyetlerde bulunulmakta, ayrıca yapılan siber güvenlik çalışmaları esnasında konusu suç teşkil eden bulgular ile karşılaşılması halinde adli makamlar ve kolluk kuvvetleri ile koordinasyon içerisinde hareket edilmektedir.

Diğer taraftan, USOM tarafından hazırlanmış olan yerli ve milli SOME İletişim Portalı (SİP) üzerinden ülkemiz siber güvenlik organizasyonunda yer alan Sektörel ve Kurumsal SOME'lere güvenlik bildirimleri, alarm, duyuru, mesaj ve ihbarlar gönderilmektedir. Aynı zamanda SOME'ler de SİP kanalı üzerinden tespit ettikleri ihbar ve olay bildirimlerini USOM'a iletebilmektedir. USOM'a gelen ihbar, olay bildirimlerin konusuna göre inceleme ve değerlendirmeler yapılarak gerekli aksiyonlar alınmakta ve aldırılmaktadır.

BTK tarafından yürütülen siber güvenlik ile ilgili çalışmaların en önemlileri arasında siber güvenlik tatbikatları yer almaktadır. Siber güvenliğin sağlanmasına yönelik girişimler içerisinde uzmanlık seviyesinin geliştirilmesi, bilgi güvenliği standartlarının uygulanması ve kullanıcı eğitimlerinin yanı sıra, siber güvenlik konusunda farkındalığın arttırılmasına yönelik çalışmalarda siber güvenlik tatbikatları önemli bir yer tutmaktadır.

Siber güvenlik tatbikatlarının amacı;

- Katılımcıların siber saldırılara karşı koyma yeteneklerini geliştirmek,
- Katılımcıların siber saldırılara karşı kurum içi ve kurumlar arası koordinasyonlarını geliştirmek ve
- Siber güvenlik konusunda ulusal farkındalık seviyesini arttırmaktır.

2011 yılından itibaren Ulaştırma ve Altyapı Bakanlığı koordinasyonunda, BTK tarafından **5 ulusal ve 2 uluslararası siber güvenlik tatbikatı** gerçekleştirilmiştir.[73]

Kişisel Verileri Koruma Kurumu (KVKK) 7 Nisan 2016 tarihinde 6698 sayılı kanunla kurulmuş olup, Kurumun amacı, anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, ülkemizde kişisel verilerin korunmasını sağlamak ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmek, aynı zamanda veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmaktır.

KVKK Kanununun amacı, kişisel verilerin işlenme şartlarını, kişisel verilerin işlenmesinde kişilerin temel hak ve özgürlüklerinin korunmasını ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir. Kişinin mahremiyetinin korunması ile veri güvenliğinin sağlanması da bu kapsamda değerlendirilmektedir. KVKK kanunu ile kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması, yetkisiz kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi amaçlanmaktadır.

TÜBİTAK: TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM), bilişim, bilgi güvenliği ve ileri elektronik alanlarında gerçekleştirdiği çalışmalarla ülkemizin ihtiyaçlarına yenilikçi ve milli çözümler üreten ulusal Ar-Ge merkezidir. BİLGEM, Türkiye'de bilgi güvenliği ve bilişim alanında teknolojik bağımsızlığı sağlamak için, askeri ve sivil bilginin güvenliğini, bütünlüğünü, güvenli bir şekilde iletilmesini ve saklanmasını sağlayan teknolojik Ar-Ge çalışmaları gerçekleştirmektedir.

[73] https://www.usom.gov.tr/

BİLGEM'in temel faaliyetlerini Araştırma-Geliştirme, Test ve Değerlendirme, Prototip Üretimi ve Eğitim oluşturmaktadır. BİLGEM ileri elektronik, bilişim teknolojileri, kriptoloji, siber güvenlik, yazılım teknolojileri, bilgi güvenliği, elektronik harp ve telekomünikasyon alanlarında bugüne kadar yüzlerce başarılı projeye imza atan enstitülere sahiptir. Bu enstitüler şu şekildedir: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE), Bilişim Teknolojileri Enstitüsü (BTE), İleri Teknolojiler Araştırma Enstitüsü (İLTAREN), Siber Güvenlik Enstitüsü (SGE) ve Yazılım Teknolojileri Araştırma Enstitüsü (YTE).[74]

3.3.2 Bilişim (Siber) Suçları ile Mücadelede Kişisel Tedbirler

Kişisel bazda alınabilecek tedbirler ise çeşitli yazılımlar, programlar veya uygulamalar aracılığıyla sağlanabilir. Bunlar;

Zafiyet Tarayıcı (Vulnerability Scanner): Bir sistemde muhtemel açıkların belirlenmesi amacıyla yapılan bir taramadır, sistemin güvenlik düzeyini ölçer. Ancak sunulan her bulgu ciddi bir zafiyet göstergesi olmak zorunda değildir. Sistem bu önemsiz açığı başka bir şekilde koruyor olabilir.

Güvenlik Duvarı (Firewall): Yerel ağ ile dış ağlar arasındaki iletişimi koruyan yazılım veya donanımlardır. Kimi zaman sadece yerel ağ içi iletişimin kontrolünü sağlamak amacıyla da kullanılabilir. Güvenlik duvarı üzerinde politikalar (rules) düzenlenerek ağlar arası ya da ağ içinde hangi verinin alınıp hangi verinin alınmayacağı belirlenebilir. Ayrıca güvenlik duvarı üzerindeki etkinlikler daha sonra incelenebilmek adına kayıt altına da alınabilmektedir.

Saldırı Tespit / Önleme Sistemi (Intrusion Detection / Prevention System - IDS/IDP): Makine öğrenmesi ile oluşturulan bu sistemler nasıl bir güvenlik istendiğine göre farklılık gösterecek şekilde programlanırlar. Örneğin tüm ağı kontrol ederek muhtemel bir siber saldırıyı önleyebileceği gibi, sunucuya gelen taleplerde çeşitli tespitlerde bulunabilir ya da herhangi bir saldırı karşısında sistemin kapatılması üzerine rapor verebileceği gibi sistemi kapatma emri de verebilir.

[74] https://bilgem.tubitak.gov.tr/tr/kurumsal/biz-kimiz

Antivirüs: Bilgisayarı ve sunucuları belirli aralıklarla tarayarak çeşitli saldırı ve tehditlere karşı koruyan, bunları fark ederek engelleyen, buna ek olarak kişisel bilgilerin güvenliğini sağlayan, virüslere karşı da güvenlik duvarı oluşturan yazılımlardır. İşletim sisteminin kararlı ve stabil çalışmasına da yardımcı olmaktadır. Bilgisayara bağlanan ek donanımları tarayarak yine bilgisayarın güvenliğini sağlarlar.

Veri Kaçağı Önleme Sistemi (Data Loss Prevention - DLP): Sistemdeki bilgilerin sızdırılması, çalınması veya herhangi bir şekilde dışarıya kaçırılması gibi durumların önlenmesi için izleme ve önleme olarak çift yönlü görevlerin yine yazılım ve donanımlar üzerinden çift yönlü şekilde gerçekleştirilmesi ile oluşan bir güvenlik sistemidir. Ağ güvenliğini sağlamak amaçlı kullanılan yöntemler arasında yeni sayılabilecek yöntemler arasında bulunmasına rağmen yaygın bir şekilde kullanımına başlanmıştır. Bu sistem istenmeyen veri çıkışını önlediği gibi dosya kullanım durumlarının izlenmesine de olanak tanımaktadır.

Yığın İleti Engelleme Sistemi (Anti Spam): Kurum, kuruluş veya bireyler fark etmeksizin istek dâhilinde olmadan zarar vermek, reklam yapmak ya da kişilerin mesajları, kredi kartı şifreleri, adres defterleri gibi hassas bilgileri çalmak amaçlı gönderilen e-postaların e-posta kutusuna düşmelerini engelleyen sistemlerdir.

İçerik Filtreleme Sistemi (Content Filter): İletişim ağları dâhilinde belirlenen kurallar çerçevesinde istenmeyen kelimeler, videolar, web siteleri, sohbet odaları gibi çeşitli içerikleri filtreleyerek belirleyen ve herhangi zararlı bir yazılım tespit ederek filtreleme sunucularına göndermesi sonucu ekranlarda engellenme sayfasının çıkmasını sağlayan sistemlerdir.

Bal Küpü (Honeypot): Zafiyet içeren sistemleri taklit ederek saldırganları yavaşlatmak ve hedef şaşırtmak amacıyla oluşturulmuş yem sunuculardır, çeşitli servisler ve istemcilerden oluşturulmaktadır. Fazlasıyla zafiyet bulunan bu sistemler aynı zamanda pasif/aktif bilgi toplayarak saldırganı kendi üzerine çekmeyi de amaçlamaktadır.

Ağ Erişim Kontrol Sistemi (Network Access Control - NAC): Bu sistem yine diğer savunma sistemleri gibi yazılımsal ve donanımsal olarak varlığını gösteren sistemlere başka bir örnektir. Kurum ve kuruluşlarda mevcut bulunan ağın güvenliğini sağlayan bu sistemler belirlenen politikalar kapsamında kaynaklara ulaşımı sağlar. Bu politikalar çerçevesinde sistemleri ağa dâhil etmek veya karantinaya almak ya da direkt olarak ağ dışına çıkarmak gibi işlemler

yapabildiği gibi karantinada bulunan sistemler için gerekli güncellemeleri yaparak ve gerekli yama güncellemelerini alarak uygun hale gelen bilgisayarların ağa tekrar katılması gibi süreçleri de yönetebilir. Bu tür ağ erişim kontrol sistemleri ajanlı ve ajansız olmak üzere ikiye ayrılır. Ajanlı ağ erişim kontrol sisteminin ajansız olanlardan farkı sistemler üzerinde daha derinlemesine ağ kontrolü yapılmasını sağlamasıdır. Bu sistemi geleneksel güvenlik sistemlerinden ayıran en önemli özellik ise ağ alt yapısını kontrol ederek kullanıcıların gerekli güvenlik politikalarını uygulayıp uygulamadıklarını kontrol edebilmesidir.

Adli Bilişim Sistemleri (Computer Forensic Systems): Elektro ve elektro optik ortamlarda bulunan bilişim sistemleri içerisindeki verilerin ses, video, veri olarak toplanması, saklanması, yedeklenmesi, imajının alınması, derlenmesi, analiz edilebilmesi amacıyla ilke ve standartlara uygun bir şekilde mahkemelerde yasal delil olarak sunulması çalışmalarıdır.

Uç Nokta Güvenliği Sistemi (Endpoint Security): Gerçek zamanlı saldırılara karşı gerçek zamanlı koruma sağlayan sistemlerdendir. Antispyware, şifreleme, ağ tabanlı saldırıları önleme, uygulama ve cihaz kontrolleri, web tehditlerine karşı koruma, veri kaybını önleme, sistem ve tarayıcı saldırılarına karşı engelleme, USB, CD cihazları kontrol etme gibi çeşitli alanlarda koruma sağlarken, kullanıcı hatalarını da kullanıcıların güvenliği lehine önlemeyi amaçlar.

Şifreleme (Kriptografi): Şifreleme bilimi olarak bilinir. Bütünlük, gizlilik, kimlik denetimi hassas bilgilerin matematiksel yöntemlerle korunması anlamına gelmektedir. Bir bilginin iletimi, ağın dinlemesi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi, bilginin göndericisi ve alıcısını arasındaki koruma amacı ile kullanılır.

Steganografi: Yunancada "gizli yazı" anlamına gelen kelime ile adlandırılan bu yöntem, taşınmak istenen bir verinin kimsenin haberdar olmadığı bir ortamda saklanarak farklı kişilerin verinin varlığından haberdar olmasını engellemek amacıyla kullanılır. Yani mesajı görülmeyecek şekilde gizler ve iletişimin gizli devam etmesine yardımcı olur. Bilgiyi sağlamak için farklı formatlardaki dosyalar kullanılarak bilgilerinde gizlenmesi söz konusudur. Günümüzde yaklaşık %95 oranında en çok kullanılan "JPG", "EXE", "BMP", "MP3", "GIF", "TIF", "DOC" "WAV", "AVI", "MPEG", "DLL", vb. dosyalar tercih edilmektedirler

Elektronik İmza / Sayısal İmza (Electronic / Digital Signature): Islak imzaların yerine de geçen elektronik imzalar imza gönderen kişiden yasal olarak emin olunmasını amaçlar ve bu yasal doğrulama sistemi ile resmi işlemlerin internet üzerinden yapılması sağlanarak zamandan ve kâğıttan tasarruf edilmesi sağlanır ve işler elektronik ortamda arşivlenerek yürütülür. Elektronik imzalar kullanıldığı kamu kuruluşlarıyla yapılan işlemlerde, bankacılık ve sigortacılık işlemlerinde, gümrük işlemlerinde e-devlet, e-iş ve e-ticaret uygulamalarında, elektronik posta ve kanun kapsamındaki hukuki işlemlerde kullanılabilir.[75]

3.3.3 Adli Bilişim

Adli bilişim sabit disk veya taşınabilir bellek gibi elektronik materyallerin içerisindeki sanal verilerin incelenmesi ve gerçek dünya ile bu veriler arasındaki ilişkinin kurulması yoluyla herhangi bir suçu ispat edecek olan dijital verilerin ortaya çıkarılması işlemidir. Burada elde edilen ve suçu ispat edebilecek dijital verilere ise dijital delil adı verilmektedir.

Dijital veriler yapıları gereği çokça değişkenlik gösterdikleri için yanlış müdahale verilerin geri dönülemez bir şekilde kaybolmasına neden olabilir. Bundan dolayı dijital delillere müdahalede bulunacak olan kimselerin bilişim sistemlerinin nasıl işlediğini, bilginin nasıl saklandığı ve iletildiğini, siber dünyanın kurallarını ve bu ortamdaki dijital delillere nasıl müdahale edilmesi veya bunları nasıl kullanması gerektiğini iyi bilen kimseler olmalıdır. Bu kimseler Adli Bilişim Uzmanlarından başkası değillerdir.[76]

Adli bilişimin amacı muhtemel yasal ve elektronik delillerin keşfedilmesi, toplanması, analiz edilmesi ve sunulmasıdır böylece suçlunun tespitinde gerekli olabilecek tüm sayısal delillerin elde edilmesi amaçlanır ve herhangi bir şekilde yorum içermez, deliller tarafsız bir biçimde sunulur. Bir çeşit teknik inceleme yöntemi olarak görev yapmaktadır.

Adli bilişim üç alt türe ayrılmaktadır. Bunlar; bilgisayar adli bilişimi, ağ ve internet adli bilişimi ile gömülü cihazlara ait adli bilişim olarak sıralanabilir. Bunlara ek olarak günümüzde sosyal ağ adli bilişimi de dördüncü bir adli bilişim türü olarak kimileri tarafından kabul görmektedir.

---

[75] ÇALIŞKAN Bülent, Siber Güvenliğin Önemi ve Alınabilecek Tedbirler, Ahmet Yesevi Üniversitesi, Yüksek Lisans Semineri, 2018: 47-48. https://www.academia.edu/40440026/Siber_Guvenli%C4%9Fin_Onemi_ve_Alinabilecek_tedbirler

[76] DÜLGER Murat Volkan, Adli Bilişim & Ülkemizde Uygulanması, İstanbul Aydın Üniversitesi, Mayıs 2017, https://www.researchgate.net/publication/318792740_Adli_Bilisim_ve_Ulkemizde_Uygulamasi

Bilgisayar adli bilişimi en çok kullanılan adli bilişim yöntemidir. Suç işlendikten sonra olay yerinde bulunan her türlü bilgisayarın adli birimlerce teknik prosedürlere ve usul kurallarına uygun olarak ön güvenliğinin sağlanması, adli bilişim laboratuvarına taşınması, bilgisayar içinde bilgi barındırabilecek tüm verilerin incelenmesi, gerekli ilişkilendirilmelerin yapılarak rapor hazırlanması ve adli makamlara sunulması sürecini kapsamaktadır. Ağ ve internet adli bilişimi suçluların bir kurum ya da firmaya ait sisteme maddi çıkar veya kişisel eğlence için sızmaları durumunda kurum ya da firmanın saygınlığının zedelenmesi sebebiyle tüm sisteme ait logların bilgisayar sunucularının ve ağ üzerinden giden paketlerin incelenmesi, gerekli ilişkilendirmelerin yapılması, raporlanması ve adli makamlara sunulması süreçlerini içermektedir. Gömülü cihazlara ait adli bilişim iPhone, Blackberry ve iPad gibi cihazlarla işlenen suçlarda bu cihazların ele geçirilmesi ve suç unsuru içerebilecek bilgilerin çıkartılması, raporlanması ve ilgili makamlara sunulması şeklinde gerçekleşmektedir. Sosyal ağ adli bilişimi Web 2.0'ın ortaya çıkmasıyla gündeme gelmiş sosyal ağlar ve paylaşım ortamları üzerinden kayıp kişilerin takibi, kötü amaçlı yazılım yayma, insan kaçakçılığı, dolandırıcılık gibi eylemlerin tespiti olarak karşımıza çıkmaktadır.[77]

Aynı zamanda adli bilişimin alt disiplinleri olarak adlandırılabilen adli bilişim yöntemleri yediye ayrılmaktadır. Bunlar; bilgisayar adli bilişimi, ağ adli bilişimi, mobil adli bilişim, GPS adli bilişim, medya araçları adli bilişimi, sosyal ağ adli bilişimi ve uzaktan arama yöntemleridir. Bilgisayar adli bilişimi temel olarak veri kurtarma üzerine çalışmaktadır. Çünkü suçluların kişisel bilgisayarları en birincil verileri barındırması bakımından en çok veri alınabilecek kaynaklar olarak işlev göstermektedirler. Ağ adli bilişimi local, wan ya da internet ağ trafiklerinin izlenmesi, analizi ve sonuçları doğrultusunda adli makamlara gerekli bilgilerin verilmesi işlemlerini kapsar. Mobil adli bilişim cep telefonları içerisinde tutulan servis sağlayıcılara ait fatura bilgileri ya da arama detay bilgilerinin elde edilmesini sağlayan bilişim disiplinidir. Suçlunun kimle, ne zaman konuştuğu gibi önemli bilgilerin yanı sıra telefon ile gerçekleştirilebilen çeşitli işlemlerden bilgi toplanabilmesini sağlar. GPS adli bilişim kiralanan araçlarda, toplu taşımalarda veya taşımacılık, nakliye vb. birçok sistemde, kişilerin favori yer bilgileri, araçların nereleri ziyaret ettiğine dair bilgiler zamanlı bir biçimde tutularak suça dair muhtemel durumların incelenebilmesini sağlar. Medya araçları adli bilişimi çeşitli bellekler, müzik oynatıcıları, ses kayıt cihazları ile kayıt altına alınan veya bunlarda taşınan çocuk

[77] ÖZEN Muharrem ve ÖZOCAK Gürkan, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi," Ankara Barosu Dergisi, Sayı: 1 (Ocak, 2015): 45-47. https://dergipark.org.tr/tr/pub/abd/issue/33821/374544

pornosu gibi bulundurulması suç olan görsel ve işitsel medyaların zaman damgalı bir şekilde kaydedildiği bu cihazların içindeki verilerin silinmesi ya da ortaya çıkarılması gerektiği zamanda görev yürüten disiplindir. Sosyal ağ adli bilişimi kişilerin sosyal ağlarda iletişim hallerindeki değişiklikler, haberleşmeler, hakaret ve tehditler, katılmış oldukları gruplar, grup hareketleri vb. birçok iletişim faaliyeti gibi durumların sosyal ağlar üzerinde tutulan verilerin incelenmesi, analiz edilmesi ve delil teşkil etmek üzere adli makamlara sunulması ile ilgilenmektedir. Uzaktan arama yöntemleri, suç delilinin var olduğu şüphesi bulunan bilişim sistemlerine uzaktan erişme sayesinde delil arama ve elde etmeyi hedefleyen adli bilişim yöntemidir.[78]

Adli bilişim inceleme süreci delil elde etme aşaması, laboratuvar incelemesi ve raporlama aşaması olarak üç kısımdan oluşmaktadır. Bu süreç olay yerinde başlar ve raporun mahkemeye tebliğ edilmesi ile sona erer. İlk aşamada dijital delilleri içeren elektronik materyaller özenli bir şekilde toplanır. Bu aşamanın titizlikle yürütülmesi diğer aşamaların daha kolay ve sağlıklı ilerlemesini sağlar çünkü doğru ve gerekli deliller mahkemenin muhakeme sürecini kolaylaştıracaktır. Olay yerinde ele geçirilen veriler işlenmeden önce bulgu niteliğindedir. Bu bulgular içerisinde delilin bulunup bulunmadığını ortaya çıkarmak adli bilişim uzmanlarının görevi dahilindedir. Laboratuvar incelemesinin ardından bulgular delil niteliği kazanırlar. Son olarak talep edilenler doğrultusunda eldeki verilerden bir rapor hazırlanır. Teknik bilgiler içeren bu rapor dikkatli hazırlanmalıdır ki gereksiz ayrıntılar işlenen suç hakkında kafa karışıklığı yaratmasın. Sonuç olarak bütün bu işlemler, süreçler ve sistemler siber güvenliği stabil tutma amacıyla uygulanmaktadır.[79]

3.3.4 COVİD 19 Salgını Döneminde Dijitalleşme ve Bilişim Suçları

Bilgi teknolojilerinde meydana gelen gelişmeler ve siber alanda oluşan yenilikler, 2020 yılı itibari ile hayatımızda yer edinen COVID-19 ile birlikte yaşam tarzlarını değişime uğratmış ve yeni bir düzen oluşmaya başlamıştır. Yaşam tarzının değişimi, teknolojik değişimler ile beraber siber alanın da toplum hayatı üzerinde etkisini giderek artırmaktadır.[80] Covid 19'un sebep

[78] ÖZEN Muharrem ve ÖZOCAK Gürkan, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi," Ankara Barosu Dergisi, Sayı: 1 (Ocak, 2015): 47-50. https://dergipark.org.tr/tr/pub/abd/issue/33821/374544

[79] DÜLGER Murat Volkan, Adli Bilişim & Ülkemizde Uygulanması, İstanbul Aydın Üniversitesi, Mayıs 2017, https://www.researchgate.net/publication/318792740_Adli_Bilisim_ve_Ulkemizde_Uygulamasi

[80] ATAKAN Mehmet, "Siber Güvenlik Risklerinin ve COVID-19 Salgınının Uzaktan Denetim Üzerindeki Etkileri" Sayı: 22 (Ocak, 2021): 27-39. https://dergipark.org.tr/en/download/article-file/1171658

olduğu karantina süreci, ülkemizde ve tüm dünyada aslında var olan bir dijital dönüşümün hızlanmasını büyük oranda tetiklemiş, işletmeler de faaliyetlerini sürdürmek için uzaktan çalışma uygulamalarına hızlı bir şekilde geçiş yapmak zorunda kalmışlardır.

Dünya genelinde ülkelerin koronavirüs salgınının yayılmasını önlemeye yönelik evde kalma uygulamaları gibi aldıkları tedbirler Türkiye de dâhil olmak üzere insanları e-ticarete yöneltmiş, bu süreçte insanlar geleneksel marketler yerine dijital ortamları kullanmaya başlamıştır. Bu süreçte online alışverişi kullanan sayısı gün geçtikçe artmakla beraber, online alışveriş yapmayı koronavirüs nedeniyle dışarı çıkmadan evde kalma zorunluluğu sayesinde öğrenenlerin sayısı da büyük oranda artmıştır. Pandemiyle daha da artan veri üretiminin, 2025'te toplam 200 zettabayt (ZB) hacme ulaşması beklenmektedir. Bu büyümeye paralel olarak veri depolama ürünleri de gelişmektedir. Kartuş ve disketlerle başlayan dışarıya depolama seçenekleri artık buluta taşınmaktadır.

Bununla birlikte, 2020 başından bu yana dünyanın dört yanındaki siber suçlular bu model nedeniyle ortaya çıkan güvenlik açıklarından faydalanarak saldırı yapabilecekleri ölçeği giderek büyütmüşlerdir. Özellikle pandemi döneminde bireylerin online alışverişe yönelmesi, kart bilgilerinin ele geçirilmesine yönelik yazılımları artırmıştır. Listenin başında siber suçluların hızlı sonuç aldıkları fidye yazılımlar gelmektedir. Covid-19 öncesinde geniş bir saldırıyla bireyler hedeflenirken, Covid-19 sonrasında bilgisayar korsanları şifrelemenin yanı sıra veri çalmakta, veriler fidye için tutulup, fidye verilmediği takdirde sızdırılma yoluna da gidilmektedir. Öte yandan, küresel siber suçların 2025'e kadar bu kaybın yıllık 10 buçuk trilyon dolara ulaşması beklenmektedir.

2021'de hazırlanan bir siber tehdit savunma raporu, şirketlerin yüzde 86'sının son 1 yılda en az bir siber saldırıya uğradığını göstermektedir. Fidye ödeyenlerin yüzde 28'inin ise verilerini kurtardığı belirtilmiştir. 2020'de yapılan saldırılar sonucunda fidye ödemelerinde yüzde 311'lik artış yaşanmıştır. 2020 ve 2021'in ilk yarısı karşılaştırıldığında, yüzde 150'lik artış bulunmaktadır. ABD Federal Soruşturma Bürosu FBI, 100'den fazla fidye yazılım türü olduğunu açıklamıştır.[81]Dünyada 2019'da 42 milyar dolar olan uzaktan çalışmaya bağlı güvenlik yazılımı pazarının 2022 yılında 53,1 milyar dolara yükselmesi beklenmektedir. Türkiye Bilişim Sanayicileri Derneği (TÜBİSAD) raporuna göre, Covid-19 ile siber saldırılar

[81] https://www.gazetevatan.com/bilim-ve-teknoloji/siber-felaket-kapida-dunyanin-en-buyuk-3-ekonomisine-denk-gelecek-1415046

ve saldırılarda yeni yazılım ile metotların kullanım oranı pandemi sonrası yüzde 35 artış sağlamıştır. Fidye yazılımı saldırılarında artış ise yüzde 60'ı bulmuştur.

2019'da 42 milyar dolar olan uzaktan çalışmaya bağlı güvenlik yazılımı harcamalarının 2022 yılında 53,1 milyar dolar olması beklenmektedir. Bu da pazarın daha da büyümesini beraberinde getirmektedir.2020 yılında 173 milyar dolar değerinde olan siber güvenlik pazarının 2026 yılında 270 milyar dolar büyüklüğe ulaşacağı tahmin edilirken, web ve e-posta güvenliği uygulamalarının en hızlı büyüyecek alanlar olması öngörülmektedir.

Diğer taraftan siber güvenlik vakalarına bakıldığında, olayların yüzde 63'ünün dikkatsizlik veya ihmalkârlık sonucunda çalışanlardan kaynaklı olduğu görülmektedir. Pandemiyle beraber artan uzaktan çalışma modellerinin ve çalışanların kendi cihazlarıyla şirket ortamına bağlanmalarının bu tarz güvenlik ihlallerinin artmasına sebep olduğu düşünülmektedir. Bu tür saldırıların artması da siber güvenliğin tüm kuruluşlar için ne kadar önemli hale geldiğini göstermektedir.

4 SONUÇ

Günümüzde bilgi ve iletişim teknolojilerindeki gelişmeler endüstri 4.0 ya da 4. Sanayi Devrimi olarak adlandırılıp dijitalleşmenin en önemli yapıtaşı olarak karşımıza çıkmaktadır. 21. yüzyıl insanı artık hiçbir şeyin eskisi gibi olmayacağı yeni bir dönemin eşiğinde olduğunun farkındadır. Alman araştırma kuruluşu Statista'nın verilerine göre 2020 yılında dünyada üretilen toplam sayısal içerik (ses, TV, radyo ve yazılı içerik) miktarı 64,2 zettabayt olup, 2025 yılına kadar bu miktarın 181 zettabayt'a ulaşacağı tahmin edilmektedir.[82] Sadece birkaç günde üretilen bilgi sayısal çağın başlama dönemlerine kadar insanlığın ürettiği toplam bilgi miktarına eşittir. Gün geçtikçe küreselleşen dijital dünyada geçmişte kalın çizgilerle çizilmiş sınırlar ortadan kalkmıştır. Bu muazzam bilgi akışı neticesinde artık fiziksel dünyanın yanında hepimizin var olmaya çalıştığı ayrı bir sanal dünya ortaya çıkmaktadır. Günümüzde akıllı telefonların, tabletlerin ve bilgisayarların olmadığı bir dünya tahayyül edilememektedir. Sayısal teknoloji devriminin eşiğinden adım attığımız modern çağda bireyler için vazgeçilmez olan sayısal teknoloji, şirketler ve devletler için de vazgeçilemez bir konuma yükselmiştir. İnternete bağlanmayan bir telefon artık ne kadar antik ise bilgi teknolojileri birimi olmayan bir şirket ya

[82] https://www.statista.com/statistics/871513/worldwide-data-created/

da bilgi ve iletişim teknolojilerine vakfedilmiş kurumları olmayan bir devlet de o kadar çağ dışı görülmektedir. İnsanlığın her sorununa artık sayısal teknolojiler ile bir hal yolu bulunulmaya çalışılmaktadır. Bilginin yayılması önündeki her engel ortadan kalkmakta, kasıtlı olarak iletişimi ve bilgi yayılımını engellemeye çalışan devletler dâhil her türlü organizasyon ise başarısız olmaktadır. Dijital çağda bilgi paylaşımından kaynaklanan fırsat eşitliği, gelişmiş ülkeler ile az gelişmiş ya da gelişmekte olan ülkeler arasındaki konvansiyonel teknolojileri kullanım açısından oluşan büyük farkı nispeten azaltmış olmakla birlikte tam olarak ortadan kaldırmamıştır. Ulusal Genişbant Stratejisi Eylem Planında yer alan ve CISCO tarafından yapılan bir çalışmaya göre 2021 yılı sonunda önceki 5 yıla göre küresel anlamda toplam internet trafiğinin 3,2 kattan fazla artacağı, 2800 Exabyte'a ulaşacağı görülmekte (707 milyar DVD hafızası) ve sonraki 5 yılda da 2,7 kata yakın artış olacağı tahmin edilmektedir.[83] Telekomünikasyon endüstrisindeki gelişmeler, küresel ekonomideki bilgi ve sermaye akışlarında devasa bir gelişim ve dönüşüm geçirmiştir. Dünyada toplam mobil veri trafiği geçtiğimiz 10 yılda 4 bin kat, 15 yıl öncesine göre ise tam 400 milyon kat büyümüştür. Statista tarafından yayımlanan istatistiklere göre 2021 yılı ocak ayı itibariyle 4,66 milyar insan (dünya nüfusunun yaklaşık %59,5'i) internete erişmektedir. İnternete erişim sağlayanlar arasında da erişim hızları açısından önemli farklar bulunmaktadır. Statista verilerine göre 2020 yılı dördüncü çeyreği itibariyle dünya genelinde sabit genişbant abonelik sayısı yaklaşık 1,18 milyar ve internete mobil cihazlar vasıtasıyla erişim sağlayanların sayısı ise 4,32 milyar civarındadır. Dünyada her an internet kullanım oranı artmaktadır. Bununla birlikte akıllı mobil cihazlar vasıtasıyla internete erişim yaygınlaşmakta ve internete erişim için öncelikli yöntem olmaya başlamaktadır.[84] Datareportal tarafından 2021 yılı temmuz ayında yayımlanan "Digital Around The World" raporuna göre Dünyadaki cep telefonu kullanıcılarının sayısı 5,27 milyar (nüfusun %66,9'sı) olmuştur. Aktif sosyal medya kullanıcılarının sayısı ise 4,48 milyara (nüfusun %56,8'i) ulaşmıştır.[85]

Büyük veri çağı olarak adlandırılan bu dönemde hayatımızın her alanı ve internet kullanan ortamlarda yaptığımız her işlem kayıt altına alınmaktadır. Elimizdeki veri miktarı ve bunu işleme hızı önceleri hayal dahi edilemeyen yeniliklerin ortaya çıkmasına neden olmaktadır. Sosyal paylaşım siteleri, arama motorları, çevrimiçi alışveriş siteleri bu şirketlerin kişisel

[83] https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2020_Forecast_Highlights.pdf
[84] https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=As%20of%20January%202021%20there,the%20internet%20via%20mobile%20devices.
[85] https://datareportal.com/global-digital-overview

verileri ve eğilimleri tespit edip kendi ticari faaliyetlerinde kullandıkları veri toplama alanıdır. Ancak bu kazanım kişisel verilerin gizliliği ve bilgi güvenliği açısından pek çok riski de beraberinde getirmektedir. Veri depolama ve işleme hızlarının çok hızlı bir şekilde gelişmesi hemen her şeyin sanal dünyada depolanması ve işlenmesi sonucunu doğurmaktadır. Bu teknolojik gelişme özel hayatın gizliliğine zarar verecek ve internet üzerinde bireyler için ciddi güvenlik açıklarına neden olacak gelişmeleri de beraberinde getirmektedir. Ülkelerin yasal düzenlemeleri ve bilinçli internet kullanımı bu riskleri en aza indirmek için düşünülen reçetelerdir. Kişisel verilerin gizliliği ilkesinin sınırları devletlerin yönetim felsefeleri ve kamuoylarının hassasiyetine göre farklılık göstermektedir. Bununla birlikte her devlet milli güvenliği ilgilendiren bir kriz anında kişisel verilerin tutulduğu veri depolarına erişmek isteyecektir. Bu manada büyük veri çağı olarak adlandırılabilecek yeni durumun etkin bir şekilde yönetilebilmesi ülkelerin önündeki önemli bir düzenleme alanı olarak karşımıza çıkmaktadır.[86]

Diğer taraftan, 2019 yılından itibaren yaşamakta olduğumuz ve tüm dünya ekonomilerini derinden etkileyen pandemi, döneminin tüm olumsuz etkilerine rağmen dijital devrimin hızlanmasına neden olmuştur. Ülkemizde elektronik haberleşme sektöründe büyüme ve gelişme süreci tüm hızıyla devam etmektedir. Özellikle elektronik haberleşme sektörüne yönelik yapılan yatırımları göz önünde bulundurduğumuzda, 2020 yılında 16,7 milyar TL'ye yaklaşan bir yatırım miktarının olduğunu görüyoruz.[87]

Yerli üretim ile halihazırda büyük çoğunluğu ithal edilen donanım ve yazılım ürünlerini, kendi imkanlarımız ile üreterek ülkemizin ihracatına ve istihdamına katkı sağlamamız gerektiği değerlendirilmektedir. Çünkü Ülkemizin 2023, 2053, 2071 hedeflerini gerçekleştirebilmesi ancak yüksek teknolojiye dayalı, yüksek katma değerli ürünler üretilebilmesinden geçmektedir. Elektronik haberleşme şebekelerimizde yerli ve milli donanım ve yazılımların kullanılması sadece ekonomik olarak cari açığın azaltılması bakımından önemli değil, aynı zamanda günümüzde ülkelerin savunma ve güvenlik politikaları açısından ilk sıralara yerleşen siber güvenlik ve bilgi güvenliğinin temini için de çok kritik bir öneme sahiptir.

[86] İnternetin Toplum Üzerine Etkileri-Dünyada ve Türkiye'de İnternetin Sosyal Etkilerinin Değerlendirilmesi, Bilgi Teknolojileri ve İletişim Kurumu (BTK), Şubat 2019

[87] Bilgi Teknolojileri ve İletişim Kurumu (BTK) 2021-3. Çeyrek Pazar Verileri Raporu https://www.btk.gov.tr/uploads/pages/pazar-verileri/ceyrek-raporu-2021-3-ceyrek-6-1-22-kurum-disi.pdf

Bilgi ve iletişim sektörlerinin, ülkemizin ekonomik ve sosyal refahına olan katkısı, kara, deniz, hava ve uzayda yürütülen savaş veya üstünlük yarışına beşinci bir cephe olarak siber ortamın da dahil olması ve siber güvenliğin son yıllarda beşinci savaş ortamı haline gelmesi, ilerleyen yıllarda iletişim altyapılarının daha da kritik hale geleceğini göstermektedir. Aslında siber ortamdaki üstünlük kara, deniz, hava ve uzaydaki üstünlüğün de teminatı haline gelmiştir.

Günümüzde bilişim teknolojilerinde ürün geliştirme çalışmaları, ülkelerin ya da ülke gruplarının siyasi amaçlarının veya politik güç savaşlarının gölgesinde kalmaktadır. Ülkelerin tüm dünyaya şebeke ekipmanları ve güvenlik ürünleri tedarik eden şirketlerle ilişkileri, bu şirketlerin farklı ülkelere karşı farklı hizmet koşulları sağlamaları gibi hususlar, neredeyse tüm uluslararası platformlarda vurgulanan, ikili ve çoklu anlaşmalara konu olan "işbirliği" çağrıları ve söylemlerinin ne kadar samimi olduğunun iyi değerlendirilmesini gerektirmektedir.

Siber saldırıların ya da casusluk faaliyetlerinin büyük bölümü yazılımlardaki açıklardan ya da bilerek bırakılan arka kapılardan yapılmakta ve yabancı menşeili yazılımlar kullanmak ülkelerin siber güvenliğini tehdit etmektedir.

Bilişim sistemleri vasıtasıyla işlenen bilişim suçları, bu alandaki yenilik ve gelişmelere paralel olarak çeşitlenerek artarken, bu suçlarla etkin bir şekilde mücadele açısından, bu suçları soruşturmada kullanılan delillerin de bu doğrultuda daha teknik ve uzmanlık gerektirir hale gelmesi elzemdir. Bu bağlamda, bir taraftan bu suçları soruşturmada yeni delillerin ikamesi açısından kanuni düzenlemeler yapılması gerekirken, diğer taraftan mutlaka bu suçları önleyici tedbirler alınmasının da uygun olacağı değerlendirilmektedir.[88]

Kurum içerisinde insan faktörüne bağlı oluşabilecek bilgi güvenliği riskleri tamamen ortadan kaldırılamasa da en aza indirilebilmesi için gerekli farkındalık faaliyetlerine önem verilmesi gerekmektedir. Zira bu konuda tüm dünyada bireyler yeterince bilgi sahibi değildir. 40 yaşından büyük olanların üçte biri, 18-39 yaşındakilerinse yaklaşık yarısı "kimlik avı" teriminin ne anlama geldiğini dahi bilmemektedir.

Bununla birlikte, Türkiye'de 3 milyonu aşkın KOBİ bulunmakta olup, KOBİ'ler Türkiye'deki işletmelerin %99,8'ini oluşturmaktadır. Saldırganların hedefindeki bu

[88] ATAKAN Mehmet, "Siber Güvenlik Risklerinin ve COVID-19 Salgınının Uzaktan Denetim Üzerindeki Etkileri" 27-39. https://dergipark.org.tr/en/download/article-file/1171658

büyük KOBİ ailesinin, siber risklerin büyüklüğü konusunda farkındalık kazanması ve yeni dünyada varlıklarını koruyabilmek anlamında önlem almaları gerekmektedir. KOBİ'lerin sadece yüzde 20'si siber risk konusunda önlem alırken kalanı buna ihtiyaç duymamaktadır. Alınan önemler ise genellikle virüs programı yüklenmesi ile sınırlı kalmaktadır. KOBİ'lerin bir siber uzmana sahip olmaması zincirleme siber saldırılara yol açmaktadır.

Diğer taraftan, yetenekli siber güvenlik uzmanlarına olan talep her zamankinden daha yüksek olup, dünya genelinde yeterli donanıma sahip eğitimli siber güvenlik uzmanlarına ihtiyaç duyulmaktadır. Ayrıca işletmeler koruma ürünlerini tercih ederken, bir taraftan da kurum içinde siber güvenlik politikası oluşturulması ve uygun politikalar geliştirilmesi önem kazanmıştır. Bu kurallar doğrultusunda, şirketlerin çalışanlarının görevlerinin net tanımlanması, siber risklere karşı bilgilendirmeler yapılması, tüm çalışanların bütün dosyalara ulaşamaması, verilere yönelik yedekleme prosedürlerinin devreye sokulması da bir önlem olarak düşünülebilir. [89]

5 ÖNERİLER

Günümüzün sürekli gelişen teknolojisi ile paralel olarak modernleşen iletişim kavramı sayesinde kişilere, şirketlere, bankalara, hastanelere ait önemli bilgiler bilgisayar ortamında tutulabilmektedir. Sayısal ortamdaki bu verilere sadece uygun yollardan erişmenin yanında aynı zamanda hukuka aykırı yoldan ulaşabilmek için de yine bilişim teknolojisi kullanılmaktadır. Bilişim sistemleri vasıtasıyla işlenen bu suçların diğer suçlara göre daha kolay ve ucuz işlenebilmesi faillerin ilgisini çekmektedir. Ayrıca siber saldırganların daha az bilgi ile daha kapsamlı alanlarda etki oluşturabilmeleri ve özellikle internet ortamı aracılığıyla saldırılar konusunda engin kaynaklara sahip olabilmeleri de saldırganları bu alana sevk etmektedir. Bunların daha da ötesinde, gerçek hayatta suç işlemekten çekinen insanlar, bilişim suçlarının kaynağının tespitinin zor hatta imkânsız olabilmesi, anonimlik, inkâr edilebilirlik gibi özelliklerinden dolayı bilişim teknolojileri söz konusu olduğunda çok rahat suç işleyebilmektedirler. Bu nedenlerle, siber ortamda oluşabilecek tehlikelere karşı elektronik cihaz kullanan herkesin bilinçli olması sağlanmalıdır. Bu da kişilerin konuyla ilgili eğitim almasıyla; yani farkındalık oluşturulması ile mümkündür.[90]

[89] https://www.hurriyet.com.tr/egitim/bilisim-suclari-ornekleri-ve-cezalari-nelerdir-bilisim-suclari-icin-nereye-basvurulur-ve-nasil-tespit-edilir-41907307

[90] GÖNEN Serkan, ULUS Halil İbrahim, YILMAZ Ercan Nurcan, Bilişim Teknolojileri Dergisi, Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, Cilt: 9, Sayı: 3, Eylül 2016 https://dergipark.org.tr/tr/download/article-file/230093

Kullanıcılar genellikle yerel hizmetleri evrensel olanlara tercih etmektedir. Çin ve Rusya gibi ülkelerde yerli sosyal paylaşım siteleri uluslararası rakiplerinden daha fazla talep görmektedir. Ayrıca yeni bir fikirle ortaya çıkan ve büyüyen her bir firmanın artık her ülkede yerel ihtiyaçlara göre düzenlenmiş birkaç muadili bulunmaktadır. Başka devletlerin kontrolünde olduğu iddia edilen ve kargaşa dönemlerinde bir Truva atı gibi kullanılma riski olan, ayrıca topladıkları verileri hangi alanlarda kullandığıyla ilgili tartışmaların olduğu yabancı menşeli sosyal paylaşım siteleri ve arama motorlarının yerli muadillerinin ortaya çıkmasının önemi ortadadır. Her ülkenin kendine özgü ahlak anlayışı, davranış kalıpları ve bunlar üzerine inşa edilen kanunları bulunmaktadır. Devletler fiziksel dünyada olduğu gibi sanal dünyada da vatandaşlarının fiillerini bu unsurlar kapsamında düzenlemek istemektedir. Ancak sanal dünyada güç dengesi fiziksel düzlemdekinden farklılık arz edebilmektedir. Ayrıca insanlar küreselleşen dünyada tüm dünyayı içine alan değer yargılarından nasiplenmektedir. Artık din ve milliyet ayrımı olmaksızın ortak insanlık değerlerinden bahsedilmekte ve internet bunun en önemli unsuru olarak görülmektedir. Hiçbir toplum teknolojinin sadece olumlu yönlerine bakıp kullanımının zararlı etkiler de doğuracağı gerçeğini inkâr eden bir düzenleyici yaklaşıma sahip değildir. Ancak internete erişimin çok daha kolay ve kapsamlı hale geldiği günümüzde dünya üzerindeki çok geniş yelpazede değer yargıları ve tercihleri olan milyarlarca insanın kendi kendilerini kontrol edeceğini düşünmek mantıklı değildir. İnternetin gelecekte ne tür yenilikler getireceğini tahmin etmek bugünden mümkün gözükmemektedir. Bu açıdan internet düzenlemeleri, düzenleyici otoriteler için dinamik bir alan olarak karşımıza çıkmaktadır. Hâlihazırda makul gözüken bazı alanlar ileride düzenleme yapılması gereken alanlar içine girebilir. Youtube'dan izlediğimiz videolar sadece milyon dolarlık elektrik faturaları olan çok güçlü sunucu merkezlerinden sunulmaktadır. İnternet teknolojisine dayanan BT şirketlerinin yatırım miktarı dikkate alındığında bu problemin çok daha ileri boyutlara geleceği görülmektedir. Bilgisayarlar insanlar için çok büyük kapasitede sayısal veri depolama alanları ve sınırsız veri işleme kapasiteleri sunmaktadır. İnsanın biyolojik sınırlarının çok üstünde olan bu kapasitenin nasıl kullanılacağına ancak insan muhakemesi karar verebilecektir. İyi ya da kötü kullanım tüm teknolojik yeniliklerde olduğu gibi insan unsuruna kalmıştır. Kötüye kullanılma potansiyeli interneti lanetlenmesi gereken bir unsur haline getirmez. Bununla birlikte ancak planlı ve akıllı kullanım, beklenen ve tüm ülke vatandaşlarının refahını arttıracak olumlu sonuçların ortaya çıkmasına neden olabilir. Sonuç olarak internet insanların, kültürlerin ve milletlerin kaynaştığı, bilginin kolayca yayıldığı dinamik bir alandır. Bununla birlikte internet her türlü gerçeğin manipüle edilerek değiştirilmesi, çocuk pornografisi dâhil her türlü istismarın alıcı bulması, etnik veya dini grupların baskıcı devletler ya da çoğunluk tarafından

tahakküm altında tutulması vb. gibi pek çok olumsuz tarafı da ihtiva etmektedir. Bu nedenle internete yönelik düzenlemelerin, teknik ve ekonomik yaklaşımların yanı sıra, internetin olumlu ve olumsuz etkilerini analiz edebilecek bir sosyal bakış açısıyla disiplinler arası metotlarla yapılması önem arz etmektedir.[91]

"Yasadışı erişim" terimi, bilişim sistemlerine ve bu sistemler üzerinde depolanan, işlenen veya transfer edilen verilerin güvenlik karakteristiklerine (gizlilik, bütünlük, erişilebilirlik) yönelik tehdit ve saldırı biçimindeki temel suçları kapsamaktadır. Bilişim suçunun işlenmemesi için de caydırıcı önlemlerin başında ceza hukuku alanında gerekli yasal düzenlemelerin yapılması ve cezai yaptırımların etkin bir şekilde uygulanabilmesi gerekmektedir. Bu kapsamda, fiili olarak işlenen suçların cezaları ile kıyaslandığında oldukça düşük kalan bilişim suçlarının cezalarının incelenerek, bu suçların ilk basamağı olan bilişim sistemine yetkisiz girişten itibaren cezaların tekrar değerlendirilmesi ve etkili hale getirilmesinin mücadele konusunda fayda sağlayacağı düşünülmektedir. Çünkü siber suçlara ilişkin mevcut kanunlar değerlendirildiğinde; bilişim alanında işlenen suçların ilk basamağı olan, bilişim sistemine girme ve kalma suçu başta TCK 244'üncü madde olmak üzere diğer suçlar için de bir ön koşuldur. Bu nedenle bu alanda yapılacak düzenlemelerin 243'üncü maddeden itibaren değerlendirilmesi gerekmektedir.

Kişisel verilerin korunması kapsamı birçok kanunda parça parça yer almaktadır. Ayrıca, uluslararası alanda işbirliğinin ve güvenliğin sağlanması için de, kişisel verilerin korunması ile ilgili kanunların uygulanmasının denetlenmesi, bu bilgilerin istismar edilmesini önleyici teknolojik tedbirlerin koordineli bir şekilde tüm kurumlar tarafından uygulanması önem arz etmektedir. Bu nedenle, kurumları koordine edecek ve denetleyecek bağımsız tek bir sorumlu kurumun oluşturulması; kişilerin, kurum ve kuruluşların görev ve sorumluluklarını belirleyen, insan hak ve özgürlüklerini ön planda tutarak, güvenlik demokrasi, gizlilik-kullanılabilirlik dengesini sağlayan bir kanunun hazırlanıp yürürlüğe girmesi düşünülebilir.

Ticari boyutun büyük bir bölümünün siber ortama en yaygın biçimiyle de internet ortamına taşındığı çağımızda, uluslararası boyuttaki kurum ve kuruluşlar yatırım yapacakları ülkeleri değerlendirirken inceledikleri en önemli kriterlerden birisi de siber güvenlik ve verilerin korunması ile ilgili mevzuatın bulunup bulunmadığıdır. Bu nedenle, ulusal refah ve itibar için öncelikle ulusal anlamda bilişim suçlarıyla mücadele ve bu kapsamda yasal mevzuatın

[91] İnternetin Toplum Üzerine Etkileri-Dünyada ve Türkiye'de İnternetin Sosyal Etkilerinin Değerlendirilmesi, Bilgi Teknolojileri ve İletişim Kurumu, Şubat 2019

gerçekleştirilmesinin, sonrasında da siber saldırıların kaynağının sınırının bulunmaması nedeniyle mücadelede uluslararası işbirliği ve mevzuatın oluşturulmasının önemi de ortaya çıkmaktadır.

Bilişim alanında işlenen suçların en hızlı değişim gösteren suç türü olduğu dikkate alınarak, bilişim suçlarıyla etkin ve süratli bir şekilde mücadele edebilmek için bilişim alanındaki gelişmeleri sürekli inceleyen ve ortaya çıkan değişiklikleri tespit eden, "Bilişim Alanında Uzman Hukukçulara" büyük ihtiyaç duyulmaktadır. Bu kapsamda, bilişim suçları ile ilgili düzenlemelerin süratli bir şekilde uygulanması ve hukuksal açıdan denetlenmesi için tam yetkili ve bağımsız Bilişim İhtisas Mahkemeleri oluşturularak, bilişim hâkimleri ve savcılarının görevlendirilmesinin söz konusu ihtiyacı büyük ölçüde karşılayabileceği değerlendirilmektedir. Çünkü bu sayede, sürekli değişen ve gelişen teknolojik imkânların ortaya çıkardığı yeni suçlarla mücadele için, belirli aralıklarla eğitimleri güncellenerek uzmanlaşmaları sağlanabilen hâkim ve savcılara sahip olunabilecektir. Söz konusu eğitim ihtiyacı; hukuk fakültelerinde seçmeli bilişim derslerinin açılmasıyla, mesleğe atandıktan sonra bu alanda uzmanlaşması uygun görülen personele üniversitelerle yapılacak protokol kapsamında yüksek lisans ve doktora eğitimlerinin verilmesiyle ya da meslek içi kurslar ile karşılanabilecektir. Bunun yanında bilişim hukukuna ilişkin nitelikli avukatların yetiştirilmesi maksadıyla barolar ve üniversiteler tarafından bilişim hukukuna ilişkin programların sayısı ve etkinliğinin artırılması güçlü bir muhakemenin yapılmasına katkı sağlayacaktır. Mevcut durumda, bilişim savcıları görevlendirilmekle beraber, bilişim alanında gerekli eğitime sahip olmadıkları ve dolayısıyla bu alanda uzmanlıklarının yetersiz olduğu, bu nedenle de çoğunlukla bilirkişi raporlarına dayanarak sübjektif kararlar verildiği görülebilmektedir. Özellikle son zamanlarda bilgi ve teknoloji tabanlı yapılan saldırıların nitelik ile miktarındaki önemli artışlarda dikkate alınarak ve bilişim suçlarına ait davalarda süratli bir şekilde karar verilmesi zorunluluğu nedenleriyle Bilişim İhtisas Mahkemelerinin kurulmasının; kurulurken ise Çocuk Ceza Mahkemeleri veya Fikri ve Sınai Haklar (Ceza) Mahkemelerinin örnek alınmasının uygun olacağı değerlendirilmektedir.[92]

Günümüzde siber güvenlik milli güvenliğin ayrılmaz bir parçası haline gelmiştir. Milli güvenlikle ilgili her alanda olduğu gibi ulusal siber güvenliğimizin sağlanmasında da yerli ve

[92] GÖNEN Serkan, ULUS Halil İbrahim, YILMAZ Ercan Nurcan, Bilişim Teknolojileri Dergisi, Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, Cilt: 9, Sayı: 3, Eylül 2016 https://dergipark.org.tr/tr/download/article-file/230093

milli ürün, kaynak ve yöntemlerin geliştirilmesi ve kullanılması önem kazanmaktadır. Bu amaçla, Ulaştırma ve Haberleşme Bakanlığı destekleriyle ve Bilgi ve İletişim Kurumu koordinasyonunda 2017 yılında kurulan Haberleşme Teknolojileri Kümelenmesi (HTK) bu konuda önemli bir girişim olarak göze çarpmaktadır. HTK'da 14 firma ve 3 mobil işletmecinin katılımıyla başlatılan ve TÜBİTAK tarafından da desteklenen "Uçtan Uca Yerli ve Milli 5G Haberleşme Şebekesi Projesi" kapsamında 5G altyapıları için kritik önemdeki çekirdek şebeke, baz istasyonu, 5G'ye özel yönetim, servis ve operasyonel yazılım ürünlerinin, yerli ve milli çabalarla geliştirilmesine çalışılmaktadır.

KAYNAKÇALAR

AB Yeni Siber Güvenlik Yasası, 2020
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

Almanya Siber Güvenlik Stratejisi
https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?blob=publicationFile

ALTUNOK Ebru, VURAL Ali Fatih, Bilişim Suçları, 2011/8
https://dergipark.org.tr/tr/download/article-file/208853

Avrupa Siber Güvenlik Örgütü
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/european-cybersecurity-organization.aspx

ATAKAN Mehmet, "Siber Güvenlik Risklerinin ve COVID-19 Salgınının Uzaktan Denetim Üzerindeki Etkileri" 27-39. https://dergipark.org.tr/en/download/article-file/1171658

Prof. Dr. AVŞAR B. Zakir, Prof. Dr. ÖNGÖREN Gürsel, Bilişim Hukuku, İstanbul 2010
https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf

Dr. BAYKARA Muhammet, Siber Suçlar ve Siber Terörizm
http://muhammetbaykara.com/wp-content/uploads/2018/04/3.Hafta-S%C4%B0BER-SAVA%C5%9E-VE-S%C4%B0BER-TER%C3%96R%C4%B0ZM.pdf

BIÇAKÇI Salih, Siber Güvenlik ve Savunma, Güvenlik Yazıları, Sayı: 42, Kasım 2019: 2-3
https://www.researchgate.net/publication/337569798_Siber_Guvenlik_ve_Savunma

BIÇAKÇI Salih, ERGUN Doruk ve ÇELİKPALA Mitat, Türkiye'de Siber Güvenlik, Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi, Sayı: 1 (Aralık, 2015): 33-34, https://edam.org.tr/turkiyede-siber-guvenlik/

Bilgi Teknolojileri ve İletişim Kurumu (BTK), İnternetin Toplum Üzerine Etkileri - Dünyada ve Türkiye'de İnternetin Sosyal Etkilerinin Değerlendirilmesi, Şubat 2019

Bilgi Teknolojileri ve İletişim Kurumu (BTK) 2021-3. Çeyrek Pazar Verileri Raporu
https://www.btk.gov.tr/uploads/pages/pazar-verileri/ceyrek-raporu-2021-3-ceyrek-6-1-22-kurum-disi.pdf

BOĞA Uğur, Bilişim Suçlarıyla Mücadele Yöntemleri, RTÜK Uzmanlık Tezi, 2011
https://docplayer.biz.tr/1053840-Bdldsdm-suclariyla-mucadele-yontemlerd.html

CSERNATONİ Raluca, European Union, Time To Catch Up: The Eu's Cyber Security Strategy, 2016
http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cyber-security-strategy/

ÇALIŞKAN Bülent, Siber Güvenliğin Önemi ve Alınabilecek Tedbirler, Ahmet Yesevi Üniversitesi, Yüksek Lisans Tezi, 2018: 47-48.
https://www.academia.edu/40440026/Siber_Guvenli%C4%9Fin_Onemi_ve_Alinabilecek_tedbirler

Cooperation Agreement Between INTERPOL and IMPACT on Cooperation in The Field of Cyber Security
https://www.interpol.int/content/download/11270/file/international%20multilateral%20partnership%20against%20cyber%20threats%20IMPACT.pdf

Department of Defense, United States of America, Cyber Strategy,
https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY SUMMARY_FINAL.PDF

DÜLGER Murat Volkan, Adli Bilişim & Ülkemizde Uygulanması, İstanbul Aydın Üniversitesi, Mayıs 2017,
https://www.researchgate.net/publication/318792740_Adli_Bilisim_ve_Ulkemizde_Uygulamasi

EHLİZ Hakan, Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi, 2019, http://nek.istanbul.edu.tr:4444/ekos/TEZ/ET001167.pdf

European Commission, EU Cyber Security Act
https://digital-strategy.ec.europa.eu/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity

European Commission, A European Agenda on Security
https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf

Europe Commission, A Digital Single Market Strategy for Europe
https://www.politico.eu/wp-content/uploads/2015/04/Digital-Single-Market-Strategy.pdf

Europe Commission, Siberde G7 İlkeleri ve Eylemi,
https://eucyberdirect.eu/content_knowledge_hu/g7-principles-and-action-on-cyber/

Forum of Incident Response and Security Teams (FIRST), Position paper on cybersecurity developments within the UN context
https://www.dfat.gov.au/sites/default/files/cyber-submission-first-forum-for-incident-response-and-security-teams.pdf

Fransa Ulusal Siber Güvenlik Ajansı
https://www.ssi.gouv.fr/en/cybersecurity-in-france/cybersecurity-strategy/

Fransa Ulusal Dijital Güvenlik Stratejisi
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf

GÖNEN Serkan, ULUS Halil İbrahim, YILMAZ Ercan Nurcan, Bilişim Teknolojileri Dergisi, Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, Cilt: 9, Sayı: 3, Eylül 2016

https://dergipark.org.tr/tr/download/article-file/230093

INTERPOL, Cybercrime threat response,
https://www.interpol.int/Crimes/Cybercrime/Cybercrime-threat-response

INTERPOL, INTERPOL Foundation for a Safer World
https://www.interpol.int/Our-partners/INTERPOL-Foundation-for-a-Safer-World

ITU, ITU Cybersecurity Activities,
https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

ITU, Role of ITU in building confidence and trust in the use of ICTs
https://www.itu.int/en/mediacentre/backgrounders/Pages/role-of-ITU-in-building-confidence-and-trust-in-the-use-of-ICTs.aspx

İngiltere Siber Güvenlik Stratejisi, 2011
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

İngiltere Siber Güvenlik Stratejisi Yıllık Raporu, 2016
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

Japonya Ulusal Siber Güvenlik Savunma Raporu, 2020
https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf

KARADAĞ Şerife, Siber Uzayda Uluslararası Hukuk Mümkün mü, Selçuk Üniversitesi, 2019 http://sssjournal.com/Makaleler/1545056113_06_5-36.ID1522_Karada%c4%9f_2827-2833.pdf

NURKULOV Nurshod, New Cyber Strategy Of China And The Alterations İn The Field, University of World Economy and Diplomacy, Özbekistan, Ocak 2017

https://www.researchgate.net/publication/322739786_New_Cyber_Strategy_of_China_and_the_Alterations_in_the_Field

OECD, Bilgi Güvenliği ve Gizlilik Politikasına İlişkin OECD Kaynakları
https://www.oecd.org/sti/ieconomy/security-and-privacy-resources.htm

OECD, OECD Dijital Güvenlik Risk Yönetimi Raporu, 2015
https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

OECD, Konseyin OECD Yasal Enstrümanları Sağlık Veri Yönetimine İlişkin Tavsiyesi
https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf

ÖNOK Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İş birliği," Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 19, Sayı: 2 (Aralık, 2013): 1232-1235. https://dergipark.org.tr/tr/pub/maruhad/issue/48280/623844

ÖZEN Muharrem ve ÖZOCAK Gürkan, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi," Ankara Barosu Dergisi, Sayı: 1 (Ocak, 2015): 45-47. https://dergipark.org.tr/tr/pub/abd/issue/33821/374544

ÖZÜDOĞRU Uğur, Siber Suçlar ve Mücadele Yöntemleri Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri, BTK Bilişim Uzmanlığı Tezi, 2011: 121-122 https://docplayer.biz.tr/57366564-Siber-suclar-ve-mucadele-yontemleriz-dunya-uygulamalari-ve-turkiye-icin-cozum-onerileri.html

PERNIK Piret, WOJTKOWIAK Jesse, KIRSS Alexander Verschoor, National Cyber Security Organisation: United States, https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf

TAŞCI Ufuk ve CAN Ali, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014," Fırat Üniversitesi Sosyal Bilimler Dergisi 25, Sayı 2 (Temmuz, 2015): 232. https://dergipark.org.tr/tr/download/article-file/157433

TÜİK, Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması 2021, 26 Ağustos 2021 https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437

TURHAN Oğuz, Siber Suçlar, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf

TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) https://bilgem.tubitak.gov.tr/tr/kurumsal/biz-kimiz

United Nations, Developments in the field of information and telecommunications in the context of international security https://www.un.org/disarmament/ict-security/

United Nations, RESOLUTION ADOPTED BY THE GENERAL ASSEMBLY https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement

YILMAZ Furkan, GÜLLÜPINAR Fuat, Türkiye'de Bilişim Suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi, https://dergipark.org.tr/tr/download/article-file/1169453

YILMAZ Sacit, 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar,

http://tbbdergisi.barobirlik.org.tr/m2011-92-669

https://tr.wikipedia.org/wiki/Bili%C5%9Fim_su%C3%A7lar%C4%B1

https://www.statista.com/statistics/871513/worldwide-data-created/

https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2020_Forecast_Highlights.pdf

https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=As%20of%20January%2020 21%20there,the%20internet%20via%20mobile%20devices.

https://datareportal.com/global-digital-overview

https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/
https://www.gazetevatan.com/bilim-ve-teknoloji/siber-felaket-kapida-dunyanin-en-buyuk-3-ekonomisine-denk-gelecek-1415046

https://www.hurriyet.com.tr/egitim/bilisim-suclari-ornekleri-ve-cezalari-nelerdir-bilisim-suclari-icin-nereye-basvurulur-ve-nasil-tespit-edilir-41907307

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF