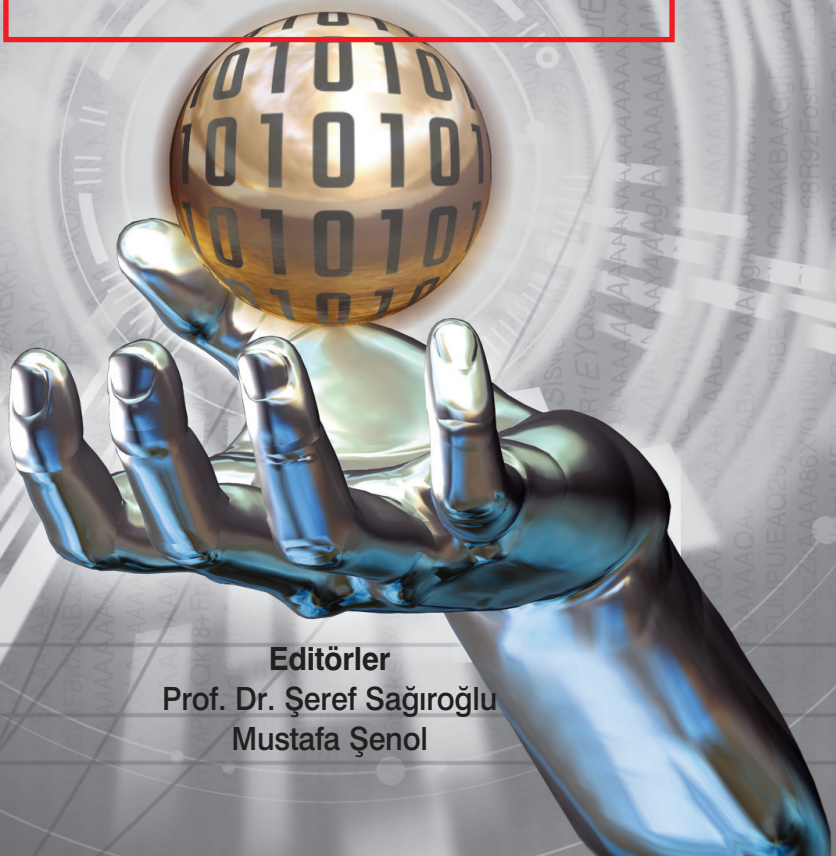
BGD Siber Güvenlik ve Savunma Kitap Serisi 2

Siber Güvenlik ve Savunma

PROBLEMLER VE ÇÖZÜMLER



Editörler
Prof. Dr. Şeref Sağıroğlu
Mustafa Şenol

Grafiker Yayınları

Siber Güvenlik ve Savunma

PROBLEMLER ve ÇÖZÜMLER

Editörler
Prof. Dr. Şeref SAĞIROĞLU
Mustafa ŞENOL

Yazarlar
Prof. Dr. Şeref SAĞIROĞLU
Prof. Dr. Ramazan BAYINDIR - Prof. Dr. Yaşar BİLGE
Prof. Dr. Türksel KAYA BENSGHIR
Doç. Dr. Sedat AKLEYLEK - Doç. Dr. Muharrem Tolga SAKALLI
Doç. Dr. Murat CENK - Dr. Öğr. Üyesi İbrahim Alper DOĞRU
Dr. Murat DÖRTERLER - Dr. Ahmet EFE - Dr. Yılmaz VURAL
Dr. Mehmet Rıda TÜR - Dr. Mehmet Bedii KAYA
Dr. Adem TEKEREK - Öğr. Gör. Seyfettin VADİ
Arş. Gör. Kübra SEYHAN - Arş. Gör. Meryem SOYSALDI
Gürol CANBEK - Murat AKIN
Hatice TOMBUL - Mehmet TUNÇKANAT

Ankara 2019

Siber Güvenlik ve Savunma: Problemler ve Çözümler

Editörler
Prof. Dr. Şeref SAĞIROĞLU
Mustafa ŞENOL

Yazarlar
Prof. Dr. Şeref SAĞIROĞLU
Prof. Dr. Ramazan BAYINDIR
Prof. Dr. Yaşar BİLGE
Prof. Dr. Türksel KAYA BENSGHIR
Doç. Dr. Sedat AKLEYLEK
Doç. Dr. Muharrem Tolga SAKALLI
Doç. Dr. Murat CENK
Dr. Öğr. Üyesi İbrahim Alper DOĞRU
Dr. Murat DÖRTERLER
Dr. Ahmet EFE
Dr. Yılmaz VURAL
Dr. Mehmet Rıda TÜR
Dr. Mehmet Bedii KAYA
Dr. Adem TEKEREK
Öğr. Gör. Seyfettin VADİ
Öğr. Gör. Murat AKIN
Arş. Gör. Kübra SEYHAN
Arş. Gör. Meryem SOYSALDI
Gürol CANBEK
Hatice TOMBUL
Mehmet TUNÇKANAT

ISBN: 978-605-2233-50-4

1. Baskı
Mayıs, 2019 / Ankara
1500 Adet

Grafiker Yayınları
Yayın No: 315
Web: grafikeryayin.com

Kapak, Sayfa Tasarımı, Baskı ve Cilt
Grafiker
Grafik-Ofset Matbaacılık Reklamcılık San. ve Tic. Ltd. Şti.
1. Cadde 1396. Sokak No: 6
06520 (Oğuzlar Mahallesi) Balgat-ANKARA
Tel : 0 312. 284 16 39 Pbx - Faks : 0 312. 284 37 27
E-posta : grafiker@grafiker.com.tr
Web : grafiker.com.tr

HAVELSAN Bu kitap HAVELSAN'ın katkılarıyla basılmıştır.

İÇİNDEKİLER

3. BÖLÜM
KRİPTOGRAFİK TEST YÖNTEMLERİ VE KRİPTOANALİZ

4. BÖLÜM
KUANTUM BİLGİSAYARLAR İLE KRİPTOANALİZ VE KUANTUM SONRASI GÜVENİLİR KRİPTO SİSTEMLERİ

5. BÖLÜM
KUANTUM BİLGİSAYARLAR SONRASI GÜVENİLİR KAFES TABANLI KRİPTOSİSTEM TEMELLERİ

6. BÖLÜM
HUKUKİ AÇIDAN BİLİŞİM SUÇLARI, SİBER GÜVENLİK, ADLİ BİLİŞİM VE GÜNCEL TEKNOLOJİLER

7. BÖLÜM
BİLİŞİM SUÇLARINDA ADLİ TIP BİLİRKİŞİLİĞİ

8. BÖLÜM
SİBER GÜVENLİKTE SİGORTALAMA

9. BÖLÜM
SİBER GÜVENLİK İÇİN SİBER YÖNETİŞİM

10. BÖLÜM
SİBER SAVAŞ VE SİBER SİLAHLAR

11. BÖLÜM
SİBER TEHDİTLERDE SON NOKTA:
İLERİ DÜZEY KALICI TEHDİTLER

12. BÖLÜM
SIZMA TESTLERİ

13. BÖLÜM
ELEKTRİK ENERJİSİ SEKTÖRÜNDE
SİBER GÜVENLİK

14. BÖLÜM
SİBER GÜVENLİK OPERASYON MERKEZİ

EDİTÖRLERDEN

Bilgi Güvenliği Derneği (BGD), kuruluşundan bugüne kadar ülkemizin **bilgi ve siber güvenliği ile savunmasının** gelişimine katkı sağlamakta, birikimini çevreye aktarmakta, bilgi güvenliği alanında açık kaynak yaklaşımını benimseyen ve bu kapsamda içerik üretilmesine ve geliştirilmesine destek vermekte, bunları yaymakta, paylaşmakta ve kamuoyunun kullanımına sunmaktadır. Düzenlediği ulusal ve uluslararası etkinliklere ait bildiri kitapları serisi, hazırladığı raporlar, taslak strateji dokümanları, eylem planları vb. bunların başında gelmektedir. **Siber Güvenlik ve Savunma Kitapları Serisi** ise BGD'nin ülkemizin siber güvenliğine önemli bir katkısıdır.

Tehditlerin, saldırıların ve açıklıkların artması, boyut ve yön değiştirmesi, farklılaşması, siber tehdit ekosisteminin gittikçe güçlenmeye başlaması, kritik altyapıların hedef haline gelmesi, bilgi ve kaynak hırsızlıklarının çoğalması, yeraltı yapıların etkinleşmesi, siber saldırıların artık savaşa dönüşmesi, siber suç ve suçlularının çoğalması, siber terörün yaygınlaşması vb. olumsuzlukların hızla artması, yapılacak mücadele, alınacak önlem ve karşı koymak için yaklaşımlara duyulan ihtiyacı artırmıştır. Kapsamlı bir mücadele için; ulusal strateji ve eylem planlarına, araştırma merkezlerine, gelişmiş altyapı ve araçlara, lisans ve lisansüstü programlara, nitelikli insan kaynağına, yerli ve milli ürünlerin geliştirilmesine, siber güvenlik ve savunma ekosisteminin oluşturulmasına, ulusal siber olaylara müdahale ekiplerinin sayısının ve niteliğinin arttırılmasına, Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kapsamının büyütülmesine, Siber Güvenlik ve Savunma Kurumu (Ajansı) gibi yapıların kurulmasına ve siber güvenliğin ulusal güvenlikle bütünleşmesine ihtiyaç vardır. Duyulan bu ihtiyacı bir nebze de olsa karşılamak için bu kitap serisi hazırlanmıştır. Bu kitap serisinde, 100'e yakın konu başlığı irdelenmektedir. Her bölümde, farklı bir konu siber güven-

lik ve savunma kapsamında ele alınmakta, değerlendirilmekte ve alınması gereken önlemlere yer verilmektedir.

Bu kitap serisinde sunulan konu başlıkları, ülkemizde bu alanda çalışan akademisyenler, uzmanlar ve çalışanlar ile paylaşılmış ve bu kitap serisine katkı sağlamaları istenilmiştir. Zamanı uygun olan, katkı vermek isteyen uzman veya akademisyenler belirlenen bir konuda bölüm yazarı olmaları için davet edilmişlerdir. Belirlenen süre içerisinde bölümlerini tamamlayan yazarlarımızın eserleri ise uygun olan ciltlerde basılmaktadır. Bundan sonraki süreçte, belirlenen diğer konular belirli sürelerde tamamlanıp takip eden ciltlerde yayımlanacaktır. Siber güvenlik ve savunmaya çok kapsamlı bir bakış sunmayı amaçlayan ve farklı başlıkları bir araya getiren bu kapsamlı eserin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

Bu kitap serimizin ikinci cildinde, 15 farklı bölüm sunulmuştur. Siber güvenliğin farklı açılardan irdelendiği bu ciltte; siber güvenliğin kapsamı ve boyutu, yapılan saldırıların türleri, alınabilecek önlemler, karşılaşılan yeni riskler ve problemlere yer verilmiş, karşılaşılabilecek risklere dikkat çekilmiş ve sonuçta alınması gereken önlemler ve yapılması gerekenler özetlenmiştir. Her bir bölüm; ülkemizde bu alana katkı sağlayan, bu alanda eğitim almış, tez hazırlamış, çalışmalar yapmış değerli akademisyen, kamu çalışanı ve üst düzey yöneticiler tarafından hazırlanmıştır. Her bir bölüm, birbirinden bağımsız olarak hazırlansa da konu bütünlüğü ve devamlılığının sağlanmasına mümkün olduğunca dikkat edilmiştir. Her bölüm editörler olarak tarafımızdan değerlendirilmiş, yazarlara konu içeriği ve başlıklarla ilgili olarak önerilerde bulunulmuş, düzeltmeler yapılması istenilmiş ve sonuçta yapılan değişiklikler dikkate alınarak bu kitap hazırlanmıştır. Kitapta yazılan bölümler tekrar tekrar kontrol edilmiş, yapılan çalışmalar ise her bölümün sonunda bölüm yazarları tarafından değerlendirilmiştir.

Bu kitabın, siber güvenlik ve savunma konusunda yapılacak çalışmalara ışık tutması, yeni çalışmaların yapılmasına katkı sağlaması, bu konuda yapılacak olan işbirliklerini geliştirmesi, bu konunun boyutunun ve kapsamının daha iyi anlaşılmasına katkı sağlaması ve en önemlisi ise bilgi güvenliği ve siber güvenlik alanında duyulan ihtiyacı bir nebze de olsa karşılaması, açık kaynak olarak sunulması ile de kaynaklara erişimi kolaylaştırıcı **bir başvuru kitabı serisi** olması beklenmektedir**. Bu eser serisi açık kaynak olarak**,

Bilgi Güvenliği Derneği internet sayfasında (www.bilgiguvenligi.org.tr) yayımlanmaktadır.

Kitap bölüm yazarlarımız; alan uzmanlıklarına göre her bir bölümü hazırlamışlar, kişisel bilgi birikimlerini hazırladıkları bölümlerde sunmuşlar, eserlerinin açık kaynak olarak yayımlanmasını kabul etmişler ve bu kitabın basımı ve dağıtımı ile ilgili olarak herhangi bir telif hakkı talep etmemişlerdir. Yazarlarımıza, bu kitap serisinin editörleri olarak çok özel teşekkürlerimizi ve şükranlarımızı sunarız.

Kitabın titizlikle hazırlanmasında, kontrolünde ve basılmasında başta yazarlarımız olmak üzere emeği geçen tüm paydaşlarımıza, kitap serisi fikrimizi hayata geçiren Bilgi Güvenliği Derneği Yönetim Kuruluna teşekkürlerimizi sunarız.

Prof. Dr. Şeref SAĞIROĞLU
BGD Kurucu Üyesi ve II. Başkanı
Gazi Üniversitesi MF Bilgisayar Mühendisliği Bölüm Başkanı
FutureTech Genel Müdürü

Mustafa ŞENOL
BGD Disiplin Kurulu Üyesi
HAVELSAN Yönetim Kurulu Başkan Vekili

BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN

Bilgi Güvenliği Derneği (BGD); 22 Temmuz 2007 tarihinde, Bilgi Güvenliği ve Siber Güvenlik alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, yerli ve milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak ve kamu-sektör-üniversite işbirliklerini geliştirmek amacı ile kurulmuştur.

BGD'nin vizyonu; "bilgi güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmaktır." BGD vizyonu doğrultusunda; tüm paydaşlarla işbirliği yaparak mevzuatın oluşturulmasında ve geliştirilmesinde aktif rol almakta, gerçekleştirdiği konferans, sempozyum, çalıştay ve eğitimler, yayımladığı rapor ve yazılar ile farkındalığın oluşmasına ve bunun davranışa dönüştürülmesine katkılar sağlamaktadır.

Derneğimiz bu kapsamda; "Ulusal Siber Güvenlik Strateji Belgesi" ve "Ulusal Siber Güvenlik Eylem Planı" hazırlanmasına öncülük etmiş, hazırladığı taslak metinler kabul görmüş ve sonuçta ülkemizin siber güvenlik stratejisi ve eylem planlarının gecikmeden yayımlanasına katkı sağlamıştır. Aynı zamanda; bu alanda nitelikli insan kaynağı yetiştirilmesi, mesleki yeterliliklerin belirlenmesi, kamu-endüstri-üniversite işbirliklerinin geliştirilmesi, kümelenme çalışmalarının başlaması gibi önemli politika ve stratejilerin oluşturulmasında etkin rol üstlenmektedir.

BGD, "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", "Ulusal Siber Güvenlik Stratejisi Çalıştayı", "Veri Merkezleri ve Siber Güvenlik Çalıştayı", "Siber Güvenlik Hukuku Çalıştayı", "Mobil Dünyada Çocuk ve Gençlerin Güvenliği Sempozyumu", "IPv6 Konferansı", "Kritik Enerji Altyapılarının Korunması Sempozyumu", "Ulusal Siber Terör Konferansı", "Siber Güvenlik Yaz Kampı" gibi

etkinlikleri düzenleyerek ve destekleyerek bilgi güvenliğine ihtiyaç duyulan her alanda çalışmalar yürütmüştür. Cumhurbaşkanlığı, Milli Eğitim Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Sosyal Güvenlik Kurumu ve Üniversiteler gibi farklı paydaşlar ile çalışmalar yürütmektedir.

BGD, **CyberMag Dergisi** ile toplumun tüm kesimlerine ulaşmaya çalışmaktadır. 2019 yılında 12'ncisini düzenleyeceğimiz "Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı" kısaca **ISCTurkey Konferansı** olarak bilinen uluslararası etkinlik ile kurulduğu günden bu yana kamu kurumları, özel sektör ve üniversiteleri bir araya getirmeyi başarmıştır.

Bununla birlikte, bilgi güvenliği ve siber güvenlik alanında **ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olan Bilgi Güvenliği Derneği**, bünyesinde oluşturulan BGD Genç ile; bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, orta ve yüksek öğrenim gören genç üyelerimizin mesleki gelişimini artırmak, siber güvenlik alanında farkındalık oluşturmak, ülkemizin siber güvenlik uzman kaynağını oluşturmak için gençlerimizin bu alana ilgisini artırmak için faaliyet göstermektedir.

ISCTurkey etkinlikleri, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve Ortadoğu Teknik Üniverstesi işbirliği ile düzenlenmekte, Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu tarafından sürekli desteklenmektedir. Bu etkinlik, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından "Avrupa Siber Güvenlik Ayı" platformu etkinliklerine dâhil edilen ilk ve tek etkinliktir. Ayrıca, düzenlendiği ilk yıldan beri ülkemizin siber güvenlik alanındaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, paydaşların eğitildiği, tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı ülkemizde bu alandaki en önemli etkinliktir.

Şubat 2019'da yeni bir yönetim kuruluyla göreve başlayan BGD Yönetimi, yapılan çalışmalara yenilerinin eklenmesi, açık kaynak olarak paylaşılacak olan çalışmaların artması ve ülkemizin bu alanda

ihtiyaç duyduğu Türkçe kaynak ihtiyacına katkılar sağlanmasını desteklemektedir.

Bu kitabın hazırlanmasında katkı sağlayan başta editörlerimize, hiç bir beklenti içerisinde olmadan bölüm yazan ve bunu kamuoyu ile ücretsiz paylaşılması konusunda destek veren saygıdeğer yazarlarımıza, destekleyicimize ve bugüne kadar ülke bilgi güvenliği ve siber güvenliğinin gelişimine katkı sağlayan BGD yöneticilerimize ve üyelerimize bu vesile ile şükranlarımı sunarım.

Bu kitap serisinin ikincisinin, ülkemiz siber güvenlik ve savunma çalışmalarına katkılar sağlaması dileğiyle.

Ahmet Hamdi ATALAY
Bilgi Güvenliği Derneği YK Başkanı

ÖN SÖZ

Günümüzde siber güvenlik, beşinci savaş ortamı olarak kabul edilmenin ötesinde tüm ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni olarak değerlendirilmektedir.

Yerli, güvenilir, yenilikçi ve yüksek kaliteli Siber Güvenlik çözümleri geliştirerek ülkemizin siber güvenliğinin sağlanmasında ana unsur; uluslararası pazarlarda güçlü ve güvenilir Siber Güvenlik teknoloji ve hizmet sağlayıcısı olmak vizyonu ile çalışmalarını yürüten HAVELSAN, ülkemizin siber uzayda güvenliğini sağlayacak bir mükemmeliyet merkezi olmak, ülkemizin yetenek ve kaynaklarının etkin kullanılmasına öncülük etmek adına var gücüyle çalışmalarını sürdürmektedir.

Bir Türk Silahlı Kuvvetlerini Güçlendirme Vakfı şirketi olan HAVELSAN tarafından hayata geçirilen Siber Savunma Teknoloji Merkezi çatısı altında siber güvenlik operasyon merkezi hizmetleri, kurumsal siber güvenlik danışmanlık ve destek hizmetleri, güvenlik analiz ve test hizmetleri, siber güvenlik eğitimleri ve yerli siber güvenlik ürünleri geliştirme faaliyetleri yürütülmektedir.

Siber güvenlik alanında ülkemizin nitelikli insan kaynağını artırmak için Türkçe kaynak ihtiyacının en az bu alanda verilen eğitimler kadar değerli olduğunun bilincinde olan HAVELSAN, bu ihtiyacı karşılamada katkı sağlayacak değerli bir yayın olarak gördüğü bu kitabı desteklemektedir.

Ahmet Hamdi ATALAY
HAVELSAN Genel Müdürü

Siber Güvenlik ve Ötesi

BÖLÜM 1

Prof. Dr. Şeref SAĞIROĞLU

SİBER GÜVENLİK VE ÖTESİ

Bu bölümde; siber tehditler, açıklıklar, saldırılar ve yaşanan problemler ile bunlara karşı alınan önlemler, yapılan gelişmeler, geliştirilen yeni yöntemler ile geleceğe yönelik projeksiyonlar güncel konu başlıkları altında değerlendirilmiş ve konu ile ilgili olarak **siber güvenlik ve ötesi** ile ilgili olarak değerlendirmelerde bulunulmuştur.

1.1. Giriş

Son 30 yıldır bilişim teknolojilerinin ve uygulamalarının geliştirilmesi konusuyla çalışıyorum, yapay zekâdan IPv6'ya, derin öğrenmeden büyük veriye, biyometriden yeni nesil ağlara, robotikten zeki modellemeye, web teknolojilerinden sanal gerçekliğe, protokollerden algoritmalara, makine öğrenmesinden nesnelerin internetine, bilgi güvenliğinden siber güvenliğe, kriptografiden steganografiye pek çok alanda akademik çalışmalar yapıyorum, yazıyorum, seminerler, konferanslar ve dersler veriyorum. Literatürü yakınen takip ediyorum. Bu teknolojilerin toplumları nasıl değiştirdiğini, geliştirdiğini ve zenginleştirdiğini, üretkenliği nasıl arttırdığını, işleri nasıl hızlandırdığını, kaliteyi nasıl yükselttiğini gördüm. Özellikle bunun farkında olan devletler ve hükümetlerde bu konuya daha fazla yatırım yaptılar. Ülkemizde de son yıllarda bilişim teknolojilerine yapılan yatırımlar artıyor. Verilen destekler ve teşvikler gerek sayı gerekse miktar olarak yükseliyor. Mevzuatlar iyileştiriliyor. Yeni mevzuatlar hayata geçiriliyor. Bilişim teknolojilerinin (BT) ve ar-ge kültürünün geliştirilmesine özel önem veriliyor. Desteklenen öncelikli alanlar arasında BT ve güvenliği geliyor. Teşvik ve destek paketleri açıklanıyor. 2023 hedeflerine erişmek için çalışılıyor ve hatta yeni hedefler belirleniyor. Bunun en önemli gerekçeleri ise BT'nin yeni bir ekonomi oluşturması ve BT olmadan gelişmenin, geliştir-

menin, büyümenin, koordine olmanın, yönetmenin, demokratikleşmenin veya zenginleşmenin mümkün görünmemesidir.

Dünyanın en büyük 10 ekonomisi içerisinde olmanın, 500 milyar dolarlık ihracat yapmanın, kişi başı milli geliri 25 bin dolara çıkarmanın yolunun bilim ve teknolojik geliştirme ve üretimden geçtiğinin hepimiz farkındayız. Bunun için, yeni hedefler belirleniyor ve gerçekleştirilmeye çalışılıyor, stratejiler ve politikalar geliştiriliyor, mevzuatlar güncelleniyor, yenileri yapılıyor ve destekler veriliyor. GSMH'den ar-ge'ye ayrılan pay arttırılmaya çalışılıyor. Bu oranın kısa sürede %6 olması sonra daha da yükseltilmesi hedefleniyor. Ar-Ge merkezleri açılması destekleniyor. Yeni üniversiteler açılıyor. Üniversitelerde araştırma yapan öğretim elemanları teşvik ediliyor. Aslında daha da fazlası yapılıyor. Bunlardan önemli olanlarının bazılarını aşağıda maddeler halinde verilmiştir. Bunlar;

- TÜBİTAK; gerek kamuda karşılaşılan sorunların giderilmesi gerekse sektörün ve üniversitelerin ar-ge ve proje yapmasını ve ürün geliştirmelerini destekliyor. Kritik alanlarda çağrılar açıyor. Pek çok alanda ar-ge projeleri geliştirilmesini, nitelikli insan kaynağı yetiştirilmesini, üniversitelerde teknoloji transfer ve geliştirme ofisleri kurulmasını, yurtdışı üniversiteler ile ortak ve ikili ar-ge proje ve çalışmalarını, öğretim elemanlarının yaptığı ulusal ve uluslararası yayınları konferanslarda sunmalarını, kendilerini geliştirmelerini ve gelişmiş laboratuvarlarda çalışmalar yapmasını destekliyor. Yeni alanlarda yurt dışına gitme ve teknoloji transferi sağlama konusunda çalışmalar yürütüyor. Yurtdışında bulunan iyi araştırmacıların ülkemize geri dönmelerini, laboratuvar kurmalarını ve öğrenciler yetiştirmelerini destekliyor. Üniversite öğrencilerine proje desteği veriyor, öğrenci yarışmaları yapıyor, ülkemizde lisansüstü programlarda okuyan öğrencilere uluslararası iyi üniversitelerde araştırma yapmalarını sağlamak için burslar veriyor. İnovasyonu ve patentleşmeyi destekliyor.
- YÖK; son dönemde üniversitelerde ar-ge çalışmalarına özel önem veriyor. Yeni programlar ve merkezler açılmasını destekliyor. 100-2000 Burs Projesi ile 100 kritik alanda her yıl 2000 doktoralı araştırmacı yetiştirilmesini istiyor hatta bunu 10.000'e çıkarmayı planlıyor. Akademik dünyanın kendini geliştirmesi ve yenilemesi için yeni projeler hayata geçiriyor. Yeni programlar

açılmasını destekliyor. Yurtdışı üniversitelere doktora sırasında ve sonrasında öğretim elemanlarını gönderiyor. Yüksek öğretimde kalitenin arttırılması için çalışmalar yapıyor. Ar-ge yapan personelin çalıştığı kurumda lisansüstü çalışma yapmasını ve bunun ürünleştirilmesini sağlamak için ASELSAN Akademi gibi dünya örneği programların açılmasını destekliyor.

- Ulaştırma ve Altyapı Bakanlığımız ise; pek çok alanda sorumluluklarını yerine getirmenin yanında siber güvenlik stratejisi ve eylem planı, e-devlet stratejisi gibi konularda sorumlu bakanlık olarak bunun koordinasyonunu yapıyor. Denetimler gerçekleştiriyor. Tatbikatlar yapıyor. Eylem maddelerini izliyor. Strateji ve eylem planlarını güncelliyor. Altyapının iyileştirilmesi için proje desteği veriyor. Yeni yapılar kuruyor.
- BTK; bünyesindeki USOM ile ülkemize yapılan saldırıları, tehditleri veya izinsiz erişimleri engeliyor. SOME'ler üzerinden açıklıkları tespit ediyor ve kapattırıyor, tehditleri yakınen takip ediyor, kurumlara gerekli uyarılarda bulunuyor. İnternetin yaygınlaşması ve güvenli kullanımı için projeler üretiyor ve faaliyetler yapıyor. Kurumlarımızın siber güvenlik bakış açısını hızla iyileştirmeye çalışıyor. Karşılaşılan tehdit risklerini düşürme çabası içerisinde, kamunun güvenli haberleşmesi için kamu.net projesini yürütüyor. Ülkemizde haberleşme altyapısının yerli teknolojiler ile gerçekleştirilmesi için 5G Kümelenmesi çalışmalarını destekliyor. Ülkemizde siber güvenlik alanını doğrudan veya dolaylı olarak etkileyen pek çok strateji hazırlanıyor, destekliyor veya koordine ediyor. Yarışmalar yapıyor. Bilgi birikimini arttırmak için kurduğu BTK Akademi ile çalışmalar yapıyor ve yapılmasını destekliyor.
- USOM; son dönemde çok başarılı çalışmalar yapıyor, tehditleri önlemede aktif rol alıyor, saldırı yapan komuta kontrol sistemlerini önceden tespit edip devre dışı bırakıyor, sektörel ve kurumsal SOME'lerdeki açıklıkları tespit ediyor ve açıklıkların kapatılmasını istiyor (Örnek olarak, 2018 yılı sonunda 28.079 açığın varlığını tespit ettiği, 400'e yakın sistemde zafiyeti belirlediği, 665 SOME'nin uyarıldığı bildirilmiştir.).
- KOSGEB; işletmeleri geliştirmek için destekler veriyor. Üniversitelerden mezun olmuş gençlere şirket açmaları için proje des-

teği veriyor. Genç girişimcilerin şirketleşmelerini teşvik ediyor. 20'nin üzerinde farklı programı destekliyor.

- Kalkınma Bakanlığı; şirketlerin uluslararası işbirliklerini geliştirme, geliştirdikleri ürünlerini fuarlarda tanıtmalarını teşvik ediyor. Üniversitelerin önemli alanlarda altyapını iyileştirme ve yenilerini kurma için destek veriyor.
- MEB; kritik alanlarda ihtiyaç duyulan kalifiye eleman açığını karşılamak üzere, yurtdışına lisans ve lisansüstü seviyede burslu öğrenciler gönderiyor hem de bunu 90 yıldır yapıyor. Bugüne kadar bu burslardan yaklaşık 20.000 uzman faydalandı. Şu anda yaklaşık 80'e yakın ülkede 1.500 farklı konuda 5.000'e yakın öğrenci önemli alanlarda lisansüstü eğitim alıyor.
- Savunma Sanayii Şirketleri; pek çok alanda yerli ve milli ürünler geliştiriyor ve özellikle roket, füze, tank, helikopter, uçak, İHA, ve SİHA'lar yapıyor. Üniversiteler ile ortak SAYP programı yapıyor. Gençler için eğitimler veriyor. Proje yarışmaları düzenliyor. Lisans öğrencilerini, haftada bir veya iki gün bünyesinde ücretli stajer olarak çalıştırıyor.

- TPE; patent kültürünün geliştirilmesine yönelik destekler veriyor. Etkinlikler düzenliyor. Ulusal ve uluslararası fuarlara katılımları destekliyor.
- TSE; siber güvenlik alanında, standartlar hazırlıyor, sertifika programları açıyor. Test merkezleri kuruyor. Sertifikalandırma yapıyor.
- Savunma Sanayii Başkanlığı; Siber Güvenlik Kümelenmesi çalışmaları kapsamında 127 şirket ile beraber çalışıyor. Farklı projeleri destekliyor. Bilgi birikimi ve deneyimlerin artmasına katkılar sağlıyor.
- Sanayi ve Teknoloji Bakanlığı; ürün, inovasyon ve teknoloji geliştirilmesini önemsiyor ve destekliyor. Açılan ar-ge merkezi sayısı 900'lere, çalışanlarının sayısının 40.000'lere ulaşmıştır. Tamamlanan ve devam eden projelerin sayısının 15.000'lere, patent müracaatları 5500'lere yaklaşmıştır. Kurulan ar-ge şirketlerinin %75'e yakını İstanbul, Bursa, Kocaeli, Ankara ve İzmir'de olup bu merkezlerin yaklaşık %23'ü BT alanında faaliyet göstermektedir.

Yukarıda belirtilen hususları ülkemizde destekleyen pek çok strateji belgesi ve eylem planı maddesi mevcuttur. Bunlar;

- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı,
- Ulusal e-Devlet Stratejisi ve Eylem Planı,
- Bilgi Toplumu Stratejisi ve Eylem Planı,
- Türkiye Yazılım Stratejisi ve Eylem Planı,
- Ulusal İstihdam Stratejisi,
- Organize Suçlarla Mücadele Ulusal Strateji Belgesi ve Eylem Planı,
- Verimlilik Stratejisi ve Eylem Planı,
- KOBİ Stratejisi ve Eylem Planı,
- Türkiye Kamu-Üniversite-Sanayi İşbirliği (KÜSİ) Stratejisi ve Eylem Planı,
- Türkiye Sanayi Stratejisi,
- Türkiye Girişimcilik Stratejisi ve Eylem Planı,
- Bölgesel Gelişme Ulusal Stratejisi,
- Türkiye Ulaşım ve İletişim Stratejisi ve
- 2018/1 nolu genelgesi ile kurulan "Yerlileştirme Yürütme Kurulu"

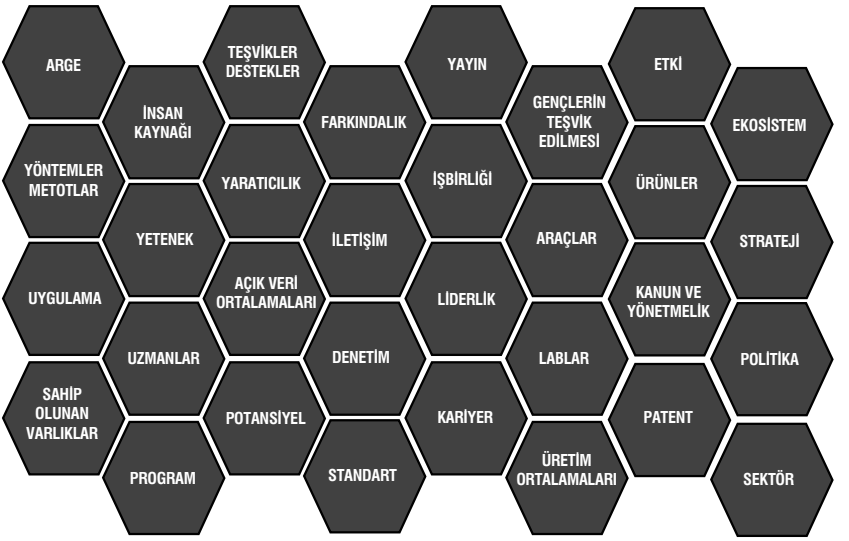
olarak verilebilir.

4691 sayılı yasa ile yürürlüğe giren "Teknoloji Geliştirme Bölgesi-TGB" ve son dönemde 5746 nolu Kanun ile hükümetin verdiği teşviklerin ve desteklerin kararlılık içerisinde sürdürülmesi ile TGB sayısı Mart 2018 sonu itibariyle 77'ye ve bu TGB'lerde kurulan firma sayısı ise 5000'lere ulaşmıştır. Bu firmaların %37'sinin yazılım sektöründe, %17'sinin BİT sektöründe faaliyet gösterdiği, bu firmalarda 50.000'e yakın kişinin çalıştığı, bunların yaklaşık 10.000'inin ar-ge personeli olduğu, 35 binin üzerinde proje üretildiği, yapılan ihracatın 3,5 Milyar dolara yükseldiği, ulusal ve uluslararası patent sayısının ise 1000'e ulaştığı açıklanmıştır. Ülkemizde üniversite başına sahip olunan patent sayısının 4,3 olduğu dikkate alındığında bu sayıların önemi daha da dikkat çekicidir.

Ülkemizdeki işletmelerin %99,9'unun KOBİ olması ve ihracatın %59,2'sini KOBİ'lerin yaptığının farkında olan Sanayi ve Teknoloji Bakanlığı; yeni fikirlerin hayata geçirilmesi, şirketleşmenin arttırıl-

ması, mevcutlarının ise büyümesi, gelişmesi, uluslararasılaşması, rekabet edebilir hale getirilmesi, kaliteli ve standartlara uygun üretim yapılması için KOBİ'lere büyük destekler vermektedir.

Sonuç olarak; yapılan çalışmalar, alınan önlemler, yapılan teşvikler, kurulan ve desteklenen altyapılar ve daha yapılan pek çok güzel işe rağmen, siber güvenlik alanında dünya örnekleri incelendiğinde, bunların sayısı maalesef yeterli seviyede değildir. ITU Global Siber Güvenlik Endeksinde ülkemiz; 2017 yılında 43. sırada iken 2018 yılı endeksinde Avrupa bölgesinde 11. dünyada 170 ülke arasında ise 20. sıraya yükselmiştir. Bu hızlı yükselişe katkı verenleri kutluyorum.



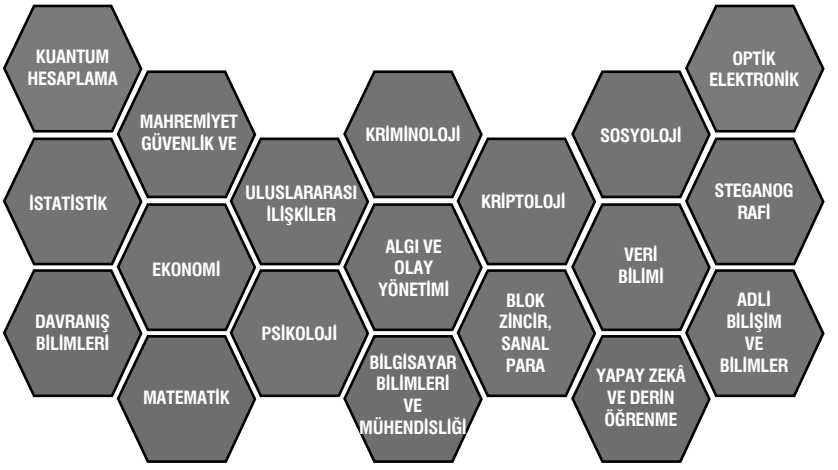
Şekil 1.1. Siber Güvenlik Ekosisteminde bulunması gereken hususlar.

Ülke bilgi ve siber güvenliğini geliştirme, önlem alma, karşı koruma sağlama kapsamlı ve çok yönlü bir iştir. Şekil 1.1, bunun kapsamını ve önemini belirtmek için verilmiştir. Şekilde belirtilen tüm hususların dikkate alınması önem arz etmektedir. Şekil 1.1'de verilen hususların ve yapılan/yapılacak çalışmaların tek bir amacı ve hedefi vardır. O da, ülkemizi bu alanda geliştirmek, milli ve yerli ürünlere sahip olmak, uluslararası standartlarda sistemlerimizi korumak ve üretim yapmak, kişisel, kurumsal ve ulusal bilgi varlıklarımızı korumaktır. Bunu sağlamak için ise Şekil 1.2'de verilen veya belirtilen hususlarda bilgi birikimine, uzmanlığa, altyapıya ihtiyaç duyulmaktadır. Belirtilen konularda ar-ge yapmaya, yeni fikirler ve teoriler geliştirmeye, inovasyon altyapılarına ve en önemlisi bunları

birleştiren, anlamlandıran, yorumlayan ve sonuçta teknolojiye, bilime ve ürüne dönüştüren insan kaynaklarına ihtiyaç vardır.

Ülkemiz siber güvenlik ve savunma konusunda hızlı bir gelişme içerisinde ise de **siber güvenlik çalışmalarının geleceği** değerlendirildiğinde;

- siber güvenlik alanında ihtisas teknoparklarının kurulması ve desteklenmesi,
- siber savunma kuluçka merkezlerinin sayısının arttırılması,
- siber güvenlik teknoloji üretimine daha çok yatırım yapılması,
- ortak test merkezleri kurulması,
- açık büyük veri ortamlarının oluşturulması ve araştırmacılara açılması,
- ar-ge merkezlerinde gençlerin fikirlerini hayata geçirebilecekleri ortamların sayısının arttırılması,
- bu bölümde anlatılan konularda daha çok çalışmalar yapılması,
- hazırlamış olduğumuz **BGD Siber Güvenlik ve Savunma Kitap Serisinde** belirtilen konular dikkate alınarak geleceğe yönelik yeni girişimlerde bulunulması, yatırımlar yapılması ve destekler verilmesi gereklidir.



Şekil 1.2. Siber Güvenlik Bilim Dalları

1.2. Farkındalığı Arttırma

Bu kitap serisinin birincisinde, farkındalığı ve bunun nasıl arttırılması ve davranışa dönüştürülmesi gerektiğini daha detaylı olarak

anlatmıştık. Burada ise "**siber güvenlik ve ötesi**" için önemli gördüğümden kısaca bir değerlendirme yapmak istiyorum. Farkındalık, her alanda sahip olunması gereken bir olgudur. Gelişmiş toplumları, toplulukları veya ülkeleri diğerlerinden ayıran bir özelliktir veya davranıştır. Farkındalık oluşturma; bilgi, dikkat, kural ve çaba ister, kültür ister, çevreye ve insana saygı ister ve en önemlisi belirlenen kurallara uyum bekler.

Siber güvenlik ve ötesi içinde aynı beklenti vardır. Bu farkındalığı oluşturmak ve geliştirmek için; tüm paydaşlar (kullanıcı, tasarımcı, geliştirici, yönetici, denetimci, araştırmacı) konunun önemini bilmeleri ve gerektiği gibi davranmaları aynı zamanda, koruma sağlama veya önlem almada tüm paydaşların işbirliği içerisinde çalışmaları gereklidir.

Siber güvenlik ve ötesini anlamak için Şekil 1.1 ve Şekil 1.2'de verilen hususlar ile bunların önemini anlamak, belirtilen bilim dallarında çalışmalar yapmak, aralarındaki ilişkileri iyi anlamak ve ilişki kurmak, ortak işbirlikleri geliştirmek, bu bilim dalları kullanılarak oluşabilecek ihlalleri tespit etmek ve yeni koruma yöntemleri geliştirmek, en önemlisi siber güvenliğe sağlayacakları katkıyı anlamak, belirtilen hususların anlaşılması için yeterli seviyede farkındalığa sahip olmak gereklidir. Mesela; bir saldırıyı anlamak için hem saldırı gerekçesini ve saldırgan psikolojisini iyi anlamak hem de bunlarla mücadele etmek için gerekli olan mevcut çözümler ile kriptoloji, matematik, davranış bilimleri, sosyoloji, olay ve algı yönetimi gibi farklı bilim dallarına ait yeni çözümler, bakış açıları, yaklaşımlar veya teknolojiler geliştirmek veya bunlardan faydalanmak gereklidir.

Farkındalığı artırmak için yapılan öneriler, aşağıda maddeler halinde verilmiştir.

1. Açıklıklar, tehditler ve saldırılar ile kullanılan teknik ve teknolojiler yakınen takip edilmeli, arkasındaki güdülenme, kullanılan metot ve metodolojiler iyi anlaşılmalı ve buna göre çözüm geliştirilmelidir.
2. Üniversitelerde ileri düzey çalışmalar, tezler, projeler ve araştırmalar yapılmalı ve bunlar pratiğe aktarılmalıdır.
3. Saldırganların; davranışları iyi bilinmeli ve analiz edilmeli, motivasyonları iyi belirlenmeli, kullandıkları yöntem, teknik ve teknolojilerin farkında olunmalı, kullandıkları veya bulunduk-

ları ortamlar izlenmelidir. Elde edilen birikimler ve deneyimlere göre de karşı çözümler geliştirilmelidir.

4. Kullanıcı davranışları, hataları, zafiyetleri ve/veya bilgi seviyesi dikkate alınarak koruma çözümleri ve koruma stratejileri belirlenmelidir.
5. Gelecek saldırıların veya gelecekte yapılacak saldırıların; daha karmaşık, farklı konuları ve bilim dallarını içerisine alan, teknik ve teknik olmayan pek çok saldırıyı kapsayacağı, içerisinde takım çalışması gerektireceği, işbirlikçi olacağı, yüksek bilgi birikimi içereceği, en önemlsi de yapay zekâ yaklaşımlarını da içeren zeki saldırılar olacağının farkında olarak, yeni teknik, teknoloji, konu, deneyim veya değişimlerin ve gelecek nesil eğilimler farkında olunarak kapsamlı çalışmalar yapılmalıdır. Her alanda, bilgi birikimi, deneyim ve yetenek arttıracak çözümler geliştirilmelidir.
6. Çözüm geliştirmenin yolu saldırı ve saldırgan verilerini analiz etmekten geçmektedir. Bunun için kurumlar arası işbirliği ve veri paylaşımı yapılması, ortak analiz çalışmaları yürütülmesi, tehdit paylaşımına önem verilmesi gereklidir.
7. Dünya siber güvenlik sektörü değerlendirildiğinde, sektörümüz belirlenen seviyede değildir. Bunun geliştirilmesi için sektöre verilen teşvikler sürdürülmelidir.
8. Siber güvenlik sağlamanın en önemli adımlarından birisi denetimdir. Sürdürülebilir denetim mekanizmaları kurulmalı, tespit edilen tehditler hızla giderilmeli ve en önemlisi gelecek ile ilgili projeksiyonlar yapılarak önlemler alınmalıdır.
9. Uluslararası işbirlikleri artırılmalıdır.
10. Çalışmaların yapılabileceği yeni altyapılar ve laboratuvarlar kurulmalı ve araştırmacılara açılmalıdır.
11. Yeni nesil saldırıların engellenmesi için özellikle yerli-milli çözümler geliştirilmelidir.
12. Farkındalık ve bilinç eksikliği, riskleri görememe veya riskleri önemsememe en önemli tehdittir. Bir kez daha vurgulamak gerekirse en zayıf halka "**insan**" dır. İnsan farkındalığını artırıcı önlemler alınmalı, eğitim faaliyetlerine önem verilmeli, farkındalık seviyeleri ara ara test edilmeli ve eksiklikler giderilmelidir. Dikkat seviyesi düşük kullanıcıların, ücretsiz olarak sunu-

lan "Güvenli İnternet Hizmetini" mutlaka kullanmaları sağlanmalıdır.

13. Kurumsal bilgi güvenliğinde yöneticilerin en çok şikayet ettikleri konuların başında; personel azlığı, personelin uzmanlık seviyelerinin yetersizliği, farklı uzmanlık alanlarına duyulan ihtiyaç, analizlerin veya testlerin istenilen ölçüde yapılamaması, müdahale takımındaki eksiklikler gibi hususlar gelmektedir. Artık bu konu hızlıca çözülmeli ve gündemden düşürülmelidir.
14. Oluşabilecek her türlü tehdidin veya zafiyetin farkında olarak, bilgi güvenliği ve siber güvenlik konusunda gerekli tedbirlerin daha dikkatli olarak alınması, kişisel, kurumsal veya ulusal olarak istenilmeyen ve arzu edilmeyen olumsuz durumlarla daha çok karşılaşılabileceği unutulmadan yukarıda belirtilen hususlar vakit geçirilmeden çözülmelidir.

1.3. Ekosistem Oluşturma

Ülke siber güvenliğinin ve savunmasının sağlanması çok yönlü bir hususdur. Bunun sağlanması için altyapıdan, insan kaynağına, yetenek birikiminden sahip olunan araçlara, kabiliyet ve kapasite oluşturmadan, yenilikçi fikir ve ürün geliştirmeye kadar pek çok husus dikkate alınmalı ve bir ekosistem kurulmalıdır. Yapay zekâ, büyük veri analitiği, veri bilimi, derin öğrenme, kuantum hesaplama, bulut hesaplama, nesnelerin interneti, blokzinciri, kriptoloji, steganografi, mahremiyet koruma, oyunlaştırma, sanal para, 5G, IPv6, dijital ikiz gibi yeni nesil teknolojiler ve yaklaşımlar ile eğitimden öğretime, planlamadan gerçekleştirmeye, tasarımdan üretime, standartlardan kaliteye, yönetimden denetime, aktarımdan dağıtıma, pazarlamadan satışa kadar pek çok alanı etkilediğinden, iyi bir siber güvenlik ekosistemi oluşturulması gereklidir. Bu ekosistemin önemli unsurlarından birisi de SSB Siber Kümelenme çalışmalarıdır. Bugün için 127'nin üzerinde şirketin bu sistem içerisinde yer alınması, bir test merkezi kurulacak olması, üniversitelilere proje yarışması açılması, eğitimler planlanması, üniversitelerle işbirliği yapılması ve ortak hedefler neticesinde yerli ve milli siber güvenlik ürünlerinin geliştirilmesinin hedeflenmesi, bu ekosistemi besleyecek önemli unsurlar arasındadır. Sağlıklı bir ekosistemin kurulması için;

- ar-ge ve inovasyon kültürü gelişmiş,
- girişimciliği yüksek,
- sadece siber güvenlik alanında değil pek çok alanda yerli ve milli üretim yapan,
- dünya ile rekabet edebilen,
- yüksek teknoloji ihracatı yapan,
- GSMH'yi yüksek olan,
- birbirine güvenen,
- devlet desteklerini ve teşviklerini yerinde kullanan ve
- verilerden değer elde eden ve bunu ekonomiye dönüştüren

yapıların kurulması veya çoğaltılması gereklidir. Ayrıca, bu hedeflere erişmek için ortak adımlar atılması, sürecin hızlandırılması, girişimciler, ürün geliştirme yolunda çaba ve emek harcayan sektör, üniversite ve kurumların desteklenmesi önem arz etmektedir. Siber kümelenmenin bu süreci hızlandırmasını, diğer küme başarılarının bu kümelenmede de kısa sürede yakalanmasını bekliyoruz.

1.4. Veri Koruma ve Mahremiyet

Mahremiyet, bu kitap serisinin birinci cildinde açıklandığı için kısaca "veri veya mahremiyet koruma", veri sahiplerinin ifşa olmaması veya sahip olunan veriden kişilere doğrudan veya dolaylı olarak erişilememesini sağlama işlemleridir.

Dünya gündemine baktığımızda, mahremiyet ihlali karşılaşılan önemli bir problemdir. Bu konu geleceğin en büyük problemlerinden birisi olacaktır. Veri toplayarak bedava hizmet veren şirketler, tüm dünyanın verisine sahip olmakta, kişilerden toplumlara, toplumlardan uluslara erişip genel modeller geliştirmektedirler. Kişisel veriler kanun kapsamında korunsa da Kanundan önce alınan veriler, mahremiyet ihlali daha büyük problemlere sebebiyet verebilecektir.

Konunun ciddiyetini gösteren bazı dünya örnekleri aşağıda verilmiştir.

- Çin, dünyada çok popüler olan sosyal medya uygulamalarının ülke içinde kullanımına izin vermemektedir.
- Facebook, bazı ülkelerde yasaklanmış bazı ülkelerde erişim engeline takılmıştır. Cambridge Analytica skandalı kapsamında 50 milyonun üzerindeki kullanıcıların kişisel verileri farklı amaçlar için kullanmıştır.

- IBM tüm çalışanlarına, USB kullanımını yasaklamıştır. Sadece bulut sistemleri üzerinden bilgi paylaşımına geçmiştir.
- Rusya, Telegram'ı yasaklamıştır.
- Almanya, Çevrimiçi Denetim Yasası ile tüm hesaplara erişebilmektedir.
- Amerika Bileşik Devletleri, tüm sosyal medya ve WhatsApp gibi haberleşme uygulamalarını Aralık 2017'den itibaren izlemektedir.
- Dünyadaki tüm akademik personelin eposta kullanıcı adı ve şifrelerini internette yayımlanmıştır.
- Facebook, Uber, vb. şirketlerin kullanıcı bilgileri ele geçirilerek internette yayımlanmıştır.
- Ülkemizdeki herkesin TC kimlik bilgileri ifşa edilmiştir.
- Kişisel ve kurumsal verilerin pek çoğu karanlık veya derin internette paylaşılmaktadır.
- AOL firması tarafından çeşitli araştırma faaliyetleri için, kullanıcı kimliği ve IP numarası silinerek belirli sayıda kullanıcıya ait 20 milyon arama sorgu verisi paylaşılmış, ancak birkaç gün içerisinde bu sorguların kimlere ait olduğu araştırmacılar tarafından tespit edilmiştir.
- Geogle, Huawei müşterilerine verdiği hizmeti durdurmuştur. Açıktan ticaret savaşlarının başladığı artık görülmektedir.

Yukarıda verilen örneklerden de açıkça görülebileceği gibi, veri göllerinin denize dönüştüğü bir dönemde mahremiyet daha fazla gündemde olacaktır. Kişisel Verileri Koruma Kurumumuz, kişisel verilerin korunması ve oluşabilecek ihlallerin kanun kapsamında incelemesi, ihlallerin belirlemesi ve yapılan ihlallerin cezalandırması konusunda gereken adımları atmakta, bilgilendirme ve farkındalığı arttırma çalışmalarını yürütmektedir.

Veri mahremiyetinin korunmasına yönelik, çeşitli anonimleştirme teknikleri ve çözümleri mevcuttur. Bu teknikler, en temelde kayıt bağlama, özellik bağlama, tablo bağlama ve olasılık saldırılarına karşı koruma sağlamaktadır. Burada verilere yapılabilecek olası saldırıların veya oluşabilecek açıkların önceden fark edilmesi veya belirlenmesi, ve sonuçta bu oluşabilecek ihlallerin engellenmesi için anonimleştirme tekniklerinin önemi büyüktür.

Verilerde anonimleştirme yapılsa da büyük veri yaklaşımlarının yaygınlaştığı, veri büyüklüklerinin arttığı ve günlük boyutunun petta bytelar seviyesine eriştiği bir dönemde, paylaşılan veri kümelerinin saldırıya ve ihlale açık olduğu bilinmektedir. Tespit edilen ihlaller, alınan kararlar ve yapılan çalışmalar bizlere yol gösterse de bugün için toplanan verilerden parmak izi gibi bir kişiyi tanımlamada kullanılan özelliklere sahip 50.000'den fazla belirleyici örüntülerin çıkarıldığı bir dönemde yaşıyoruz. Gelecekte daha çok ihlallerle karşılaşılmaması için mahremiyet çalışmalarına önem verilmeli, büyük şirketlerin veya elinde kişisel veri barındıran şirketlerin, mahremiyeti koruma adına şeffaflaşmaları için yeni çalışmalar yapılmalı, mahremiyete daha çok önem verilmelidir. Ayrıca, üzerinde durulması gereken diğer önemli bir husus ise toplumsal bazda oluşacak mahremiyet ihlalleri içinde önlemler alınmalı ve çalışmalar yapılmalıdır. Bir toplumun, grubun veya ulusun sahip olduğu toplumsal veya ulusal mahremiyetin ihlal edilmesi farklı tehditleri de beraberinde getirmektedir. Bu hususlar dikkate alınarak, karşı çözümler geliştirilmelidir.

1.5. Tatbikatlar

Tatbikatlar; kurumların, sistemlerin ve ülkelerin siber saldırılara karşı hazır olma, saldırılara koordineli olarak karşı koyma, zayıflıkları ve zafiyetleri önceden tespit etme, farkındalığı arttırma, kabiliyet ve yetenekleri birleştirme ve güçlendirme, oluşabilecek riskleri görme ve önceden önlem alma için yapılmaktadır. Ülkemiz bu konuda 4 ulusal ve 1 uluslararası tatbikat ile azımsanmayacak deneyime sahiptir. Bunlara ilave olarak askeri alanda da tatbikatlar yapılmaktadır. Bunların sonuncusu ise NATO Siber Koalisyon Tatbikatıdır. Bu tatbikatların çoğunu izleyen bir uzman olarak gözlemim, ilk tatbikatlara göre gerek içerik ve yetenek gerekse koordinasyon ve işbirliği açısından son yapılanların daha iyi ve kapsamlı olduğudur. NATO, ITU, ENISA gibi kurumlar ile Amerika, İngiltere, İsviçre, Hindistan, BAE, Moldovya'da benzer tatbikatlar yapmaktadır. 2018'de yapılan ENISA Siber Tatbikat Avrupa, APCERT Siber Tatbikat, ITU Siber Tatbikat–ALERT, Moldovya Siber Hafta, Hindistan IDRBT, BEA TRA Tatbikatı gibi dünya örnekleri incelendiğinde, konuya dünyada çok önem verildiği, haftalar ve aylar düzenlendiği, değerlendirmeler yapıldığı, dersler çıkarıldığı, raporlar hazırlandığı ve paylaşıldığı, ve yeni aksiyonlar alındığı görülmektedir. ETH

Zürih Güvenlik Çalışmaları Merkezinin 2018'de yayımladığı "CCS Siber Güvenlik Raporu" buna iyi bir örnektir.

Bugüne kadar katıldığım bu tür etkinliklerde gördüğüm ve ülkemiz kurumlarının/sektörünün kendi bünyesinde alınan ve dikkate alması gerektiğini düşündüğüm bazı hususları burada paylaşmak istiyorum. Bunlar;

- Karşılaşılabilecek tehditlere karşı hazır olmak için takım çalışmalarına, koordinasyona, bilgi paylaşımına, farklı ve yeni konularda uzmanlıklara ihtiyaç olduğundan yeteneklerin geliştirilmesi, kapasitenin attırılması, yeni araştırma altyapıları kurulması mevcutların ise iyileştirilmesi ve en önemlisi pek çok farklı konuda kapasite ve yetenek birikimlerine ihtiyaç vardır.
- İnternete bağlanıldığında dünyaya açık bir hedef olduğunun farkında olunması, her zaman bir tehdit veya saldırı ile karşı karşıya kalınabileceği veya sistemlerin zafiyete uğratılabileceği bilinciyle önlemler alınmalıdır.
- Kurumsal/sektörel SOME'lere önem verilmesi, ekiplerin eğitilmesi, yeteneklerin arttırılması, kapasitenin büyütülmesi ve en önemlisi her kurum/şirketin mutlaka bünyesinde bir SOME kurması gereklidir.
- Karşılaşılan her türlü açık veya ihlal, alınan saldırı, karşılaşılan tehdit USOM'a bildirilmeli veya koordineli çalışılmalıdır.
- Bir kriz durumunda, haberleşmenin ve gizliliğin ihlal edilmeden sürdürülmesi önem arz ettiğinden, gereken planlamalar önceden yapılmalıdır.
- Kritik alanlarda daha çok akademik çalışma yapılmalıdır. Yapılacak yayınlarda kişisel, kurumsal ve ulusal güvenliğini ihlal edecek bilgilere yer verilmemesine dikkat edilmelidir.
- Siber güvenlik tatbikat ve eğitim merkezleri kurulması, üniversite-sektör-kurumların ortak çalışmalar yapabileceği ortamların oluşturulması gereklidir.
- SSB Siber Güvenlik Kümelenmesi çalışmaları içerisinde tatbikatlara da yer verilmelidir.
- Ülkemizde ulusal farkındalığı artırmak ve tatbikatları daha geniş bir zamana yaymak için AB ülkelerinde olduğu gibi Ekim ayı "Ulusal Siber Güvenlik Savunma Ayı" olarak belirlenmeli-

dir. BGD'nin de bu yönde bir YK kararı olduğunu da belirtmekte fayda vardır.

- Etkin mücadele ve koordinasyon için uluslararası hukuk konusuna daha çok önem verilmelidir.
- Tatbikat raporlarının ETH Zürih Raporunda verildiği gibi kamuoyu ile paylaşılması da yerinde olacaktır.

1.6. Açık ve Büyük Veri Yaklaşımları

Etkin bir siber güvenlik ve savunma kapasitesi oluşturulması, verilerin analizi, yorumlanması, örüntüler ve çıkarımlar elde edilmesi, çıktılar üretimesi ve sonuçta verilerden değer elde edilmesine bağlıdır. Bunun en önemli adımı ise verilerin anonimleştirilmesi ve açık veri haline getirilerek kullanıma açılması gereklidir.

Açık Bilgi Vakfı (Open Knowledge Foundation); açık veriyi "herhangi bir telif hakkı, patent ya da herhangi bir kontrole tabi olmaksızın herkes tarafından ücretsiz ve özgürce kullanılan veri" olarak ve açık devlet versini ise "devlet ya da devlet kontrolündeki birimler tarafından üretilen, herkes tarafından kullanılabil ve paylaşılabilen veriler" olarak tanımlamaktadır. Açık veri felsefesini iyi anlamak, ve getirilerinden faydalanmak gereklidir. Devletlerin ve kurumların şeffaflaşması, işbirliklerinin artması, güven duygusunun gelişmesi, bilgi toplumu ve ekonomisinin oluşturulması, siber güvenlik ekosistemin güçlendirilmesi, tehditlerin fırsata dönüştürülmesi ve en önemlisi verilerden yeni çıktılar ve değerler üretilmesi bu felsefenin sağlayacağı önemli katkılardandır.

Dünya ülkeleri değerlendirildiğinde;

- gelişmiş ülkelerin kamu verilerini anonimleştirdiği ve kamuoyunun bilgisine ve kullanımına açtığı,
- üniversitelerin ve araştırma kurumlarının bu verilerden değer elde etme, yeni fikirler ortaya çıkarma, çıktıları ekonomik değere dönüştürme gibi benzeri pek çok konuda önemli çalışmalar yaptıkları,
- bunun ekonomisinin olduğunun farkında olarak çalışmalar yaptıkları ve kamu kaynaklarında istismarın önlenmesinde önemli kazanç elde ettikleri ve en önemlisi ise
- tüm bu işleri ise verileri anonimleştirdiklerinden kişisel verilerin korunmasına saygı göstererek yaptıkları

bilinmektedir. Ülkemizde KVKK dolayısıyla Kamu verileri açmada hep bir çekince içerisindedir. Hatta anonimleştirme ve ar-ge faaliyetleri için KVKK'da istisnalar olsa da bunu bile göz ardı etmektedirler. Mutlaka ülkemizde de açık veri felsefesinin yaygınlaşması gereklidir. Bunun için dünya örneklerinden mutlaka faydalanılmalıdır.

Açık veri ortamlarının ve platformlarının oluşturulmasında Başba- kanlığın "Açık Veri Paylaşım Portalının Oluşturulması" ve "Kamu Verilerinin Açık Veriye Dönüştürülmesi ve Paylaşılması" adımla- rının kurulan yeni yapı içerisinde kısa sürede tamamlanması, üni- versite ve araştırma kurumlarının yurtdışı açık veri portallarından aldıkları verilerle analiz yapmaları ve yurtdışına değer üretmelerinin önüne geçilerek insan kaynaklarımızın verimli ve ülke için kullanılmasının önünü açmaları, ülkemizin verilerinden değer elde edilerek ülkenin kalkınmasına ve sektörün gelişimine bunların sunulması veya önündeki engellerin kaldırılması beklenmektedir.

Ülkemizde büyük veri alanında son yıllarda yapılan akademik çalışmaların belirli bir olgunluğa geldiği görülse de açık veri konusunda yapılan çalışmaların, içerik ve derinlik olarak yeterli seviyede olmadığı değerlendirilmektedir. Bu konuya daha çok önem verilmeli ve kapsamlı ve ufuk açıcı akademik çalışmalar yapılmalıdır.

Dünya örnekleri ve çalışmaları dikkate alındığında, anonimleştirme için yeteri kadar metot ve metodolojilerin bulunduğu, oluşabilecek ihlaller konusunda çalışmaların yapıldığı, bu alanda yöneticileri ikna edecek gerek akademik çalışmaların gerekse ticari ürünlerin mevcut olduğu, bu birikimlerden de faydalanılması için gerekli adımların vakit geçirmeden atılması gerektiği değerlendirilmektedir.

2012 yılından beri Açık Yönetim Ortaklığı Girişimi (Open Government Partnership) ülkemiz tarafından desteklenmektedir. 23 Ağustos 2013'te 352013/9 sayılı ve "Açık Yönetim Ortaklığı Girişimi" konulu Başbakanlık Genelgesi[1] yayımlayarak buna taraf olduğumuz ve kurumlarımızın bu konuda gereğini yapmaları bildirilmiştir. Gelinen noktaya bakıldığında ise ülkemizde yeni

1 http://www.resmigazete.gov.tr/eskiler/2013/08/20130823-8.htm

yeni kurumların bu konuya ağırlık verdikleri ve gerekli adımları atmaya çalıştıkları, özellikle de 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı gereği de bu hususu yerine getirmeye çalıştıkları bilinmektedir. Strateji dokümanında, 22 yerde "açık veri" 24 yerde ise "büyük veri" kelimesi geçmektedir. Strateji dokümanı ve eylem planında belirtilen hususların hayata geçirilmesi beklenmektedir.

2016 yılında yayımlanan Kişisel Verileri Koruma Kanununda [7] anonimleştirme, "kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi", kişisel veri ise "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Bu tanımlara dayanarak, kişisel veri sınıfına giren büyük verilerin mahremiyeti, belirtilen kanun çerçevesinde gerek işlenmesi ve saklanması gerekse aktarılması veya ifşa edilmesi konularında aşağıda verilen iki husus dikkate alınmalıdır.

a) Büyük veri anonimleştirme alt yapısına sahip olan kurumlar

Büyük veri anonimleştirme işlemleri ve teknikleri, uzman bilgisi, deneyimi ve yüksek bilgi birikimi gerektiren unsurlardır. Bu konuda, donanım ve yazılım gereksinimleri ile nitelikli personel istihdam edilmesi anlamına gelmektedir.

Kanun; belirtilen bazı istisnai durumlar çerçevesinde veriyi işleyebilme ve paylaşabilme yetkisi vermiştir. Yedinci Bölüm "İstisnalar" başlığı altında yer alan Kişisel Verileri Koruma Kanunu Madde 28 (1-b)'de; *"Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi"* ifadesine dayanarak bir kurumun sahip olduğu verilerini anonim hale getirerek araştırma, planlama ve istatistik gibi amaçlarla paylaşabilmektedir. Burada gerek ve yeter ön şart ise verilerin anonim hale getirilmesidir. Kurumun, kendi bünyesinde büyük verileri anonimleştirme altyapısına ve uzmanlığına sahip olduğu varsayılmaktadır. Ancak, ülkemizde büyük veri sahibi olup aynı zamanda o veriyi anonimleştirecek veya bunun gereklerini karşılayabilen bir kaç kurum vardır. Diğer kurumların ise şu anda bir girişimde bulunmamasının ise pek çok gerekçesi vardır. Bunlar;

- değer üretilebilecek verilere sahip olunmaması,
- altyapı ve personel eksikliği,

- risk almama,
- KVKK
- bilgisizlik, ilgisizlik ve çekinme,
- üçüncü taraflara güvensizlik,
- iyi örneklerin bulunmaması veya
- diğer bazı haklı sebepler olabilmektedir.

b) Büyük veri anonimleştirme alt yapısına sahip olmayan kurumlar

Büyük veri anonimleştirmesi için gerekli altyapı, uzman ve tecrübeye sahip olmayan kurumlar ise bu ihtiyaçlarını bir şekilde karşılamak durumundadır. Bu durumda, akla gelen ilk çözüm gerçek veya tüzel kişilerden hizmet alımıdır.

KVKK'nın Yedinci Bölümü, İstisnalar başlığı altında yer alan Madde 28 (1-c)'ye göre kanun hükmünün aşağıdaki madde uyarınca uygulanamayacağı belirtilmiştir.

Kişisel Verileri Koruma Kanunu Madde 28 (1-c)'de *"Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi"* ifadesine dayanarak sanat, tarih ve bilimsel amaçlarla işlenebileceği, ayrıca kanunun İkinci Bölüm Kişisel Verilerin Aktarılması başlığı altında yer alan Madde 8 (a ve b)'de verilerin aktarılması hususu şu şekilde belirtilmiştir. *"Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması halinde, ilgili kişinin açık rızası alınmadan aktarılabilir"* ifadesine dayanarak çeşitli hükümler çerçevesinde kişisel verilerin aktarılabileceği görülmektedir. Burada önemli olan durum, 6 ncı maddenin üçüncü fıkrasında belirtildiği üzere sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca işlenebileceğidir. Bu duruma göre, büyük veri anonimleştirme altyapısına sahip olmayan kurumlar ile imzalanacak gizlilik sözleşmesi çerçevesinde, kurumlar "hizmet veya danışmanlık alımı" yolu ile anonimleştirilmesi istenen büyük verilerin gerçek veya tüzel kişilerin veritabanlarına aktarılabileceği değerlendirilmektedir. Bu kapsamda aşağıdaki iki madde veri işleme ve paylaşmanın hangi doğrultuda olması gerektiği gösteren yönlendirici maddelerdir.

- Madde 5 (2-f) – *"İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"*
- Madde 6 (3) – *"Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir"*

Bu konuda dünyadaki yeni yaklaşımlardan da haberdar olunma- sında fayda vardır. ABD'de kurulan ve büyük şirketlerin daha ileri ve güvenliği üst düzeyde sağlayan araç, gereç ve yazılımlar geliş- tirilmesi ve mevcutlarının kalitesinin artırılması için Siber Tehdit Birliği (Cyber Threat Allience) kurulmuştur. Bu kurumlar birbirleri arasında verileri paylaşmakta ve bu veriler ile ürünlerinin kalitesini, verimliliğini, başarısını ve en önemlisi güvenlikte yeni bakış açısı geliştirilmesi için kullanılmaktadır. Ülkemizde rekabetçi ürünler geliştirilmesi, daha güvenli ortamlar oluşturulması, kaynakların verimli kullanılması, güvenlik açığı oluşturacak risklerin önceden belirlenebilmesi için bu gibi örneklerin farkında olunması benzer yaklaşımlar geliştirilerek kişisel verilerin korunmasına da dikkat edilerek geleceğe dönük çalışmalar yapılması ve çözümler geliştirilmesi gereklidir.

1.7. Geleceği Etkileyen Teknolojiler

Siber ortamlar Şekil 1.1 ve 1.2'de de verildiği gibi içerisinde pek çok bilim dalını ve konuyu içermektedir. Bunları bilmek, aralarındaki ilişkileri anlamak, siber güvenliğin yüksek seviyede sağlanmasında bunlardan nasıl faydalanılacağının farkında olmak, aralarındaki etkileri ve etkileşimleri öngörmek, geliştirilen teknikleri, teknolojileri, modelleri, yöntemleri veya çalışmaları iyi anlamak ve kavramak ve bunlardan en iyi şekilde faydalanmak, işin teorisine ve felsefesine odaklanmak gereklidir.

Bu bölümde, geleceği ve gelecekteki güvenlik bakış açılarımızı geliştirecek yeni teknolojiler tanıtılacak ve gelecekte karşılaşılabilecek riskler, olası önlemler ve elde edilebilecek üstünlükler sunulacaktır.

1.7.1. Yapay Zekâ ve Derin Öğrenme

Yapay Zekâ (YZ) 65 yıldır gündemde olan bir konudur. Son dönemde veri miktarının artması, problem uzayının büyümesi, veri depolama ve işleme teknolojilerinin geliştirilmiş olması, dağıtık yapıda veri işleme teknolojilerinin ilerlemiş olması, büyük veri analitiği ile derin öğrenme yaklaşımlarının veri işlemeye büyük bir boyut kazandırması ve en önemlisi elde edilen başarılı örneklerin çoğalması ile YZ tekrar gündeme oturmuş bir konudur.

Kendi içerisinde YZ kavramı bile değişmektedir. Artık, "genelleştirilmiş yapay zeka (AGI)" yaklaşımlarına odaklanılmaktadır. Bu yaklaşım; pek çok yeni teknolojileri, yöntemleri, algoritmaları, yapıları, çözümleri ve uygulamaları içerisinde barındırmaktadır. Bunlar, gelecekle ilgili ümitlerimizi ve beklentilerimizi artırmaktadır. Bunun gerekçeleri ise son dönemde YZ çalışmalarında alınan yol, geliştirilen uygulamalar, elde edilen başarı oranları, bu yapıların artık kendi dillerini geliştirebilmeleri, otonom olarak çalışabilmeleri, başarılı şekilde tercüme yapabilmeleri, güvenlik sistemlerinde otomatik olarak alarm üretebilmeleri, gösterilen resimleri anlatabilmeleri, konuşmaları anlamlandırabilmeleri, kelimelerdeki farkı anlatımları çıkarabilmeleri, duyguları anlayabilmeleri, tek başına olduğu kadar topluca kişileri tanımlamaları, kişilikleri ve karakterleri analiz edebilmeleri, kullanıcıları düşünce olarak sınıflandırabilmeleri, otomatik zeki saldırılar düzenleyebilmeleri veya yapılan saldırıları anlayıp zekice karşı koyabilmeleri, yazıları ve resimleri anlamlandırabilmeleri, karmaşık sistemleri öğrenebilmeleri, farklı sistemlerle entegre olabilmeleri, farklı durumlara uyum sağlayabilmeleri, öğrenebilmeleri, matematiksel olarak modellenemeyen sistemleri modelleyebilmeleri, donanım olarak gerçekleştirilmelerinden dolayı hızlı işlem yapabilme kabiliyetine sahip olmaları gibi özellikler YZ'yı öne çıkarmaktadır.

Yapay zeka artık; üniversitelerin, şirketlerin, resmi kurumların, inovasyona gönül verenlerin, istihbarat servislerinin, askeri birliklerin vazgeçemediği çözümler sunmaktadır. Tercih edilmelerinin gerekçeleri ise "problemleri zekice çözme", "yüksek kazançlı ve gelir getirici olma", "yeni fikirlerin hayata geliştirilmesini kolaylaştırma", "yenilikler sunma" ve "büyük resimleri görmemize katkı sağlama", "güvenilir sistem yaklaşımı sunma", "öğrenebilme", "hemen hemen her alana uygulanabilme" ve en önemlisi "yüksek performanslı çözümler sunma" gibi yapıları desteklemeleridir. Bundan dolayı;

- YZ'ye yatırımlar yapılmakta ve teşvikler verilmektedir.
- YZ adında bakanlıklar açılmaktadır.
- YZ enstitüleri kurulmaktadır.
- YZ Mühendisliği bölümleri açılmaktadır.
- YZ artık yeni meslekler ortaya çıkarmakta ve diğer alanlardaki çalışmaları da etkilemektedir.
- YZ çok farklı alanlara kolaylıkla uygulanabilmektedir.

Bunların sayısı arttırılabilir. Mesela, YZ'nın en iyi kullanıldığı alanlardan birisi de güvenliktir. Olası tehditlerin belirlenmesi, otomatik tehdit algılama, tehditlere karşı koyma, anormal davranışları belirleme, belirli bir örüntüyü bulma, yapılan saldırıların seviyesini anlama, tehdit seviyesini belirleme, saldırı davranışını öğrenme, belirli saldırıların modellerini anlama, saldırıları modelleme, yeni saldırı oluşturma gibi pekçok alanda başarıyla kullanılmaktadır. Bundan sonra; saldırılara otomatik olarak karşı koyma, yapılan ihlalleri otomatik olarak belirleme, yapılabilecek olan ihlalleri önceden belirleme ve engelleme, zafiyetleri belirleme ve önleme gibi alanlarda YZ'nin katkısını artık daha sık duyacağız ve göreceğiz, bu teknolojilerden daha fazla faydalanacağız, hayatımızı kolaylaştırdığını daha çok hissedeceğiz ve bu teknolojileri daha sık kullanacağız.

Günümüzde ise bu konuya verilen önemi göstermek için Sophia ile YZ'nin geldiği nokta anlatılmaya, paylaşılmaya, gösterilme- ye, cilalanmaya veya pazarlanmaya çalışılmaktadır. Robotlara duygusallık kazandırılarak robotların "aşık olup olmayacağı", "insanlığı yok edip edemeyeceği", "gelecek için bir tehdit olup olmayacağı" ve "etik davranıp davranmayacağı", "mahremiyeti ihlal edip etmeyeceği", "bizim gibi düşünüp düşünmeyeceği" veya "bizden daha zeki olup olamayacağı" gibi hususlar da sorgulanmaktadır.

Elon Musk yapay zekâyı "insanlığın geleceği için en büyük tehlike" olarak görmekte ve YZ'nin "insanoğluna bir gün hükmedeceğini" düşünmektedir. Bunu ileri düzeye taşıyanlar da vardır. YZ çalışmalarının bir an önce durdurulmasını istemektedirler. Google ve Facebook gibi büyük şirketler buna çok yatırım yapmışlardır. Fakat elde edilen sonuçlar ve bunların toplum ve uluslar üzerinde oluşturduğu olumsuz örnekler, karşı karşıya kalınan olaylar, bu konunun ciddiyetini bizlere göstermek için yeterlidir. Mesela; Facebook'un 50 milyonun üzerinde kullanıcı verilerinden çok farklı analizler yapa-

rak kişilerin mahremiyetini ihlal etmesi, bu ve buna benzer pek çok olayla kolaylıkla karşılaşılabileceğinin bir göstergesi olmuştur. Bu analizlerde pek çok bilim dalından faydalanılmış olsa da en önemli destekleyici unsur ise YZ yaklaşımlarıdır.

Google'ın ABD Savunma Bakanlığı ile yürüttüğü MAVEN isimli 8,6 milyon dolarlık Yapay Zeka Projesini sürdürmeme kararı alması, bu yüzden işten ayrılan çalışanların olması, bu projeye karşı olanların sayısının hızla yükselmesi, İHA görüntülerinden kişileri otomatik olarak tanıması, bunu savaş teknolojileriyle birleştirip kullanması gibi sebepler bu fitili ateşlemiştir. Google sunduğu pek çok hizmetle artık tekelleşmeye giderken "kullanıcılarını daha çok korkutmaktan" çekindiği için "savaş teknolojileri ticaretinden" uzak durma eğiliminde olduğunu gösterme çabası içerisine girmiştir. Ayrıca, başlatılan karşı imza kampanyasına katılımların artması, dörtbinin üzerinde imza toplanması, bazı Google çalışanlarının yapılanları etik bulmamaları, bazılarının ise işlerinden istifa etmeleri de bunu tetiklemiştir.

Doktorasını YZ üzerine yapmış, bu konuda çalışmalara devam eden bir akademisyen olarak, 25 yıl önce konuştuğumuz pek çok husus ancak bugün yapılabiliyor, hayata geçirilebiliyor veya gerçekleştirilebiliyor. Çalışmalar ağır gitse de gelinen nokta bize bundan sonraki süreçlerin daha hızlı olacağını göstermektedir.

YZ'nin gelecekte sorun olacağı veya oluşturacağı aşikar ama YZ yaklaşımları ile bugün karşılaşılan problemlere çözümler geliştirilse de gelecekte karşılaşılabileceğimiz pek çok problemin daha olmadan veya oluşmadan çözümlenmesi mümkün olacaktır. Karşılaştığımız pek çok sıkıntının ise gelecekte bu teknolojiler sayesinde yaşanmayacağı da ortadadır. Zeki çözümler hayatımızın pek çok alanında yer alacaktır.

Bugün için YZ konusunda odaklanması gereken hususun; topluma, insanlığa faydalı, hukuka saygılı, çevreye duyarlı yeni teknolojiler, algoritmalar ve yapılar geliştirilmesi ve bunları da karşılaşılacak problemleri çözmede kullanmaktır. Yapılan her işte risk olduğu gibi YZ'nin gelişiminde de beklenmedik hususlar her zaman olacaktır. Überin sürücüsüz aracının kaza yaparak ve bir kişinin ölümüne sebebiyet vermesi gibi örnekler bizleri temkinli davranmaya itmektedir. Bu tür olaylara karşı hazır olmak veya bunları ortadan kaldırmak için çalışmalara devam etmek gereklidir.

Ülkemizde yapay zeka çalışan bilim insanlarına da bu konuda büyük sorumluluklar düşmektedir. Sevindirici olan husus yapay zeka konusunda yapılan pek çok çalışma vardır. Yeterli sayıda bilim insanı bulunmaktadır. Hatta, hiçbir üniversitemiz dünyada ilk 100'e girememiş iken, Yapay Zeka Biliminin gelişmesine katkı sağlayan kurumlar sıralamasında dünyada Erciyes Üniversitesinin 82. sırada olması gurur vericidir. Bu gibi başarılar iyi kullanılmalı ve bu bilim alanının ülkemizde geliştirilmesi için özel çaba sarf edilmeli, yeni teknik ve teknolojilerin geliştirilmesine çaba harcanılmalı, yeni merkezler açılmalı, altyapılar ve laboratuvarlar kurulmalı ve mevcut olanlar ise iyileştirilmeli ve geliştirilmelidir.

Sonuç olarak; ülkemizde bilgi güvenliği ve siber güvenlik sektörünün gelişmesi yeni çözümler geliştirilmesine, bu alana yapılacak yatırımlara, oluşturulacak laboratuvarlara, kurulacak veri merkezlerine, verilerin analizi ve verilerden değer elde edilmesine bağlıdır. Üniversitelerimizde YZ ile ilgili çalışma grupları olması ve bazı laboratuvarların bulunması sevindirici olsa da ulusal düzeyde henüz bir araştırma merkezimiz maalesef bulunmamaktadır. Yayımlanan raporlarda YZ sektör büyüklüğünün bugün için 5 milyar dolar civarında olduğu ve önümüzdeki 3-5 yıl içerisinde 100 Milyar dolarlara çıkacağı da dikkate alındığında, YZ'nin sektörde, ürünlerde ve yapılan işlerde sağlayacağı katkılar ve zorlayacağı değişimler bugünden dikkate alınmalı, ülke milli güvenliğine katkı sağlayacak konuların başında olacak stratejik konulardan birisi olacağının farkında olunarak çalışmalar yapılmalı, konuya daha çok önem verilmeli, ülkemizin bu pazardan daha çok faydalanması için adımlar atılmalı ve en önemlisi geleceğe hazır olunmalıdır.

1.7.2. Nesnelerin İnterneti (Endüstri 4.0)

İlk kez 1999 yılında gündeme gelen bu terim günümüzde en çok kullanılan terimlerden birisi haline gelmiştir. Veri dünyasının gelişmesi, verilerin işlenmesi için uygun altyapı ve teknolojilerin geliştirilmesi beraberinde pek çok yeni teknolojinin üretilmesini kolaylaştırmıştır. Sensör teknolojileri de popüler konuların başında gelmektedir. Nesnelerin İnterneti, birbirleriyle belirli bir protokol üzerinden haberleşen, bilgi paylaşan, kontrol edilebilen cihaz topluluklarından oluşan ağa verilen isimdir. Bu ağ, günümüzde her alana uygulanabilen bir yapı haline gelmiş olup, sanayiden tarıma,

enerji sistemlerinden ev otomasyonuna, lojistikten sürüş konforuna, sağlıktan otomotive, savunma sektöründen askeri sistemlere pek çok alanda karşımıza çıkmaktadır.

Pazarı da doğru anlama adına bir otomasyon firması; 2020 yılında internete bağlı kişi sayısının 4 Milyar, pazarın 4 Trilyon Dolar, 25 Milyonun üzerinde uygulama, 25 milyarın üzerinde gömülü ve akıllı sistem ve 50 Trilyon GB verinin toplanacağını tahmin etmektedir. Nesnelerin internetine bağlantılı cihaz sayılarının gelecek yıllarda hızlı artacağı da öngörülmektedir.

2017 yılında nesnelerin interneti üzerinde yapılan ilk siber saldırıdan sonra konuya verilen önem artmış ise de doğası gereği tasarımda karşılaşılan kısıtlardan dolayı bünyelerinde hala güvenlik açıklıklarını barındırmaktadırlar.

Nesnelerin interneti siber uzayı daha da genişletecektir. Yapılacak saldırılar çeşitlilik kazanacaktır. Gelecek yıllarda bu ağların büyümesi de göz önüne alındığında bu konuda da çalışmalar yapılması ve gelecek tehditlere hazır olunması gereklidir.

1.7.3. Sanal Para ve Blokzinciri

Sanal paralar, dijitalleşen dünyada değişimin ve dönüşümün önemli aktörlerinden birisidir. Satoshi Nakamoto tarafından geliştirilmiş olan Bitcoin (BTC), 2008'de hayatımıza girmiş, hiçbir finans kurumunun yönetmediği, P2P protokolünü kullanan ve merkezi olmayan bir sanal paradır.

Sanal paralar, yapılan işlemleri P2P protokolü ile birbirine bağlı bilgisayarlar üzerinde blokzinciri yapısında tutarlar. Bugün için borsada işlem gören 1500'e yakın farklı sanal para bulunmaktadır. Bu yapılar, sağladıkları API'ler aracılığı ile kendi altyapı ve para birimlerini kullanan başka yazılımlarında geliştirilmesi için ortamlar sağlamakta, kendisini bir blokzinciri uygulama platformu olarak tanımlamakta ve yeni uygulamalar geliştirilebilmesinin önünü açmaktadır.

Son yıllarda en hızlı artan, en çok kazandıran/kaybettiren BTC, sadece kişilerin değil ülkelerin bile artık ulusal kriptopara birimleri haline gelmiştir. Estonya, BTC'yi ulusal para birimi olarak kabul etmiştir. Bunu diğer ülkeler izlemiştir. 2017'de ABD Miami'de araç

kiralamada BTC kullanıldığını bizzat gördüm. Fidye yazılımlarında para tahsil etmede kullanılan para birimi olduğunu hep beraber öğrendik, bazılarımız da bunun kurbanı oldular. Belki de zarara uğramayanlar olarak karşılaşılan tehditlerin boyutunun çok farkında olamadık. Ama saldırganlar, bu paralar üzerinden haksız kazanç elde ettiler. Son kullanıcılar, bu sayede iyi bir kazanç kapısı veya hedef haline gelmiştir. BTC, maalesef bu saldırıları teşvik eden bir para birimine dönüşmüştür.

Ülkemizde de bu alana ilgi duyan kullanıcılar, madenciler, şirketler ve araştırmacılar bulunsa da genel olarak bakıldığında bu alandan kazanç elde edilebilen ve ülkemize katma değer sağlayabilecek yapılar henüz beklenen düzeyde değildir. Yapılan akademik çalışmalar araştırıldığında, 3 tez, 26 bildiri, 2 proje, 23 makale ve 1 kitabın Türkçe olarak yayımlanmış olması, üniversitelerimizin konuya henüz beklenen ilgiyi göstermediğini ortaya koymaktadır.

BTC adresi sahiplerinin açıkça tanımlanmadığı göz önüne alındığında; bu tür işlemlerin anonim olarak yürütülmesi, yasadışı faaliyetleri ve işlemleri cezbetmesi, yasadışı işlemler için bir araç olarak kabul edilmesi, son dönemde fidye yazılımı mağdurlarının sayısının dünyada yüzbinlere çıkması, ulusal olduğu kadar işin uluslararası boyutunun olması, düzenleyici kurumlar ve yetkililerin yerinde uyarılar yapmasının haricinde henüz çözümler üretememesi veya üretmeye başlamamaları ülkelerde karşılaşılan temel sorunlardır.

Ülkemizde bu gibi yeni teknolojiden faydalanmak, yeni kazanımlar elde edebilmek, bilgi ekonomisine bu çalışmaları katmak işin en önemli adımı ve üstünlüğü olsa da karşılaşılabilecek olumsuzlukların da farkında olunması, karşılaşılabilecek tehdit ve tehlikelerin öngörülmesi, bununla ilgili önlemler alınması gereklidir. Bunun için; üniversitelerimizin bu konuya daha çok önem vermeleri, dijitalleşme ve kriptopara ile değişen dünyanın argümanlarını araştırıp, inceleyip, anlayıp, kullanıp, uygulayıp, yeni fikirler, teknolojiler ve çözümler üretmeleri, ve en önemlisi karşılaşılabilecek olumsuzlukları öngörülüp yeni bakış açılarının geliştirilmesine ihtiyaç vardır. Ayrıca; BTC ve blok zinciri teknolojileri yaygınlaştıkça, sıfırgün saldırılarının arttığı, güvenlik açığı sömürüsünün çoğaldığı, hizmet reddinin yanı sıra küçük blokzinciri sistemlerine yönelik saldırılarda artış olduğu, bu teknolojilerin hem bir tehdit hem de bir tehlike

oluşturma potansiyeli olan teknolojiler olduğunun farkında olunması gereklidir.

- Ülkemizde de bu alanda oluşabilecek suçları ve suçluları tespit edebilmek adına, EGM Siber Terörle Mücadele Daire Başkanlığının bu konuya önem verdiği, oluşabilecek tehdit ve tehlikeleri anlama, algılama ve önleme adına çalışmalar yaptıkları, 2018 yılında düzenlediğimiz IBIGDELFT 2018 Konferansında yaptığı sunumlardan görülmüştür. Bu tür çalışmaları, başta üniversitelerimiz olmak üzere, diğer kurumlarımızın da yapması yerinde olacaktır.
- Sektörün son dönemde blokzinciri teknolojileri geliştirme konusunda çok iyi uygulamalar, projeler ve ürünler geliştirmeye başladığını duymak ve görmek ise ayrıca çok sevindiricidir. Bunun artarak devam etmesi gereklidir.

1.7.4. Sosyal Medya

En büyük sosyal medya olan Facebook'un kurucusu Mark Zuckerberg'i bilmeyen, tanımayan, zekâsına ve yaptıklarına hayran olmayan, verilen hizmetleri beğenmeyen, sunduğu yüksek kaliteli hizmetleri takdir etmeyen yoktur herhalde. Yaşarken filmi yapılan nadir milyarder işadamlarından birisidir. Hiçbir ürün satmadan ve verilen hizmetlerden hiç para almadan milyar dolarlık şirketler kurmak herkese nasip olmuyor bu dünyada. Dünyanın en büyük şirketlerinden birisinin patronu olan Zuckerberg'in gelişen ve değişen dünyayı çok iyi anladığını ve çevresindekileri buna inandırdığı görülüyor. Temel felsefesinin, yaptığı işi en iyi yapmak, kullanıcıları buna inandırmak, kullanıcıların paylaşımları, ağları, verileri, ürettiği veya paylaştığı içerikler, istatistikler, tıklamalar, davranış modelleri, beğeniler ve sonuçta kişisel verilerin analizi ve analitiği üzerinden şirketine değer katmak olduğu anlaşılıyor.

Sosyal medya ortamlarını incelediğimizde, aslında bu ortamların kullanıcılara neler sunduğunu, kullanıcılardan neler aldığını, hizmet sayılarını ve kalitesini nasıl arttırdığını biliyoruz. Bilerek veya bilmeyerek bu ortamlarda her türlü verilerimizi paylaşıyoruz. Bu hizmetlerin ücretsiz veriliyor olması ise belki de işin en çarpıcı tarafıdır.

Facebook'un; kişisel verileri toplandığını ilk günden biliyoruz. Bu verileri kullanarak; kişileri, toplumları ve uluslarası analiz edeceği-

ni, bu verilerden para kazandığını yıllardır konuşuyoruz ve anlatıyoruz. Cambridge Analytica (CA) Skandalı ile pek çok olumsuzluk ve yapılan ihlaler su yüzüne çıktı. Artık herkes verilerinin kullanıldığından emin oldu. 50 Milyon Facebook kullanıcısının kişisel verilerinin, kişilerin bilgisi olmadan ABD seçimlerinde kullanılması ile patlak veren bu skandal tüm dünyayı bir nebze de olsa uyandırdı. Sosyal medya uygulamaları ile toplanan verilerin, aslında toplumların seçimini değiştireceği, geleceğini etkileyeceği, yaptıklarıyla yönlendirilebileceği de somut olarak ispatlandı. Çok daha fazla neler yapılabileceğinin artık farkına varıldı. Sadece dünya değil ABD bile Facebook'un gücünün farkında, neler yapabileceğini çok iyi biliyor.

Öncelikle bunun farkına varan Avrupa ülkeleri, GDPR'ı devreye almış, büyük şirketlerin veri toplama ve bunları suiistimal etmelerinin önünü kapatmak için bu adımları atmıştır. Facebook'a ve Google'a büyük cezalar kesilmiştir. Kesilmeye de devam etmektedir. Google'ın başkalarına ait verileri yayımlaması için telif alması gerektiği ise ABD'ye karşı uygulanan son hamledir. Ülkemizde ise kişisel veri ihlali yapan Facebook'a KVKK, 350'ye yakın Türk Vatandaşının veri mahremiyetine dikkat etmediği için 1.6 Milyon TL ceza kesmiştir.

Ülkemizde Kişisel Verileri Koruma Kanunu ve Kurulu devreye girdi olayın ciddiyetini ağır ağır öğrenmeye başladık. Kanunda "kişinin açık rızası" ve yapılacak olan işlerin açıkça kullanıcıya bildirilmesi gerekmekte olduğunu öğrendik. Yurt dışına çıkarılan verilerin neler olabileceği ve bunun nasıl yapılacağı, ülkelere verilebilecek zararların boyutunu gördük. Bundan sonraki süreçlerde bundan nasıl zarar görebiliriz gibi konulara artık daha çok kafa yoruyor ve çözümler geliştirmeye çalışıyoruz.

Facebook veri ihlalinin gerek kullanıcılar gerekse toplumsal bilinci, farkındalığı ve tepkiyi artırmaya başladığını görmek ise bizleri de sevindirmiştir. Mesela; "GetContact" uygulamasına tepki gecikmedi ve bununla birlikte kişisel verileri kişinin açık rızası olmadan toplayan 70'e yakın mobil uygulamaya erişim engeli geldi. KVKK-BTK işbirliği yaparak anında bu sorunu çözdüler. Artık bu uygulamalara erişim engeli var. Kurumlarımız, artık vakit geçirmeden birlikte çalışıyor ve gerekeni hemen yapıyor.

Peki bundan sonra oluşabilecek böyle olaylar karşısında nasıl bir tepki göstereceğiz? Kişisel verilerimize nasıl sahip çıkacağız? Zuckerberg'in sözüne inanacak mıyız? Bu konuyu daha fazla düşünmeli ve kişisel verilerimize sahip çıkmalı ve bunun sonucu olarak kişisel, kurumsal ve ulusal bilgi varlıklarımıza duyarlılığımızı arttırmalı, gösterilen bu tepkinin buna benzer olaylar olmadan gösterilmesi ve ihlallerin önlenmesi için bugünden çalışmamız, tehdit ve tehlikelerin farkında olmamız gerekmektedir.

Kişisel Verileri Koruma Kurulunun, 6698 nolu Kanun kapsamında ülkemizde farkındalık oluşturmak için her ilde seminerlere başlaması, Kanun gereği bu ve buna benzer olaylar karşısında gerekli reaksiyonu göstermesi, bundan sonraki süreçlerde de sadece kişisel değil ulusal reaksiyonun da gösterilmesi gereklidir.

Warren Buffett'in "siber saldırıların, nükleer bombalamalardan daha tehlikeli olduğu" gibi bir öngörüsünü dikkate almamız gerektiğini düşünüyorum. Kişisel, kurumsal ve ulusal bilgi varlıklarının sızdırılması, oluşacak ihlallerden dolayı karşılaşabileceğimiz tehdit ve tehlikeler, bunlara karşı alınabilecek tedbirler üzerinde daha çok çözüm geliştirilmesi gerektiği artık bir gerçektir.

Kişisel veri mahremiyetini sağlamayan toplumlarda ulusal mahremiyet sağlanamayacağı dikkate alınarak, gelecekte oluşabilecek toplumsal ve ulusal mahremiyet ihlalleri konusunda yeni çözümler geliştirilmeli ve önlemler alınmalıdır.

1.7.5. Bulut Ortamlar

Bulut ortamlar, kullanıcıların hizmetlerini uzaktan ama belirli bir merkez yapı içerisinden almalarını sağlayan, kullanımı kolay uygulamalar ve hizmetler sunan, kişisel bilgiler ve dosyaların güvende olduğundan emin olunan fakat sunduğu fırsatlar kadar da bünyesinde güvenlik riskleri barındıran yapılardır.

Kullanılan çözümlere bakıldığında ise; sanal sunucu sayılarının zaten fiziksel sunucuların sayısını geçtiği de bir gerçektir. Üniversitelerde, işyerlerinde, işletmelerde ve verilen hizmetlerde artık sanal sunucular hizmet vermektedir. Verilen hizmetlerin çoğu sanallaşmaya başlamıştır. Bunun haklı sebepleri de vardır. Çünkü;

- İşletim giderleri düşüktür.
- Kurulum ve değişim kolay ve hızlıdır.

- Hizmet kalitesi yüksektir.
- Ölçeklendirilebilmektedir.
- Her zaman ve her yerden erişim mümkündür.
- Enerji tüketimleri düşüktür.
- Yedekleme işlemleri kolaylıkla yapılabilmektedir.
- Yeni çözüm ve teknolojiler kolaylıkla eklenebilmekte ve güncellenebilmektedir.

Bunların sayısını artırmak mümkündür ama güvenlik sorunu hala gündemdedir. Problem olmaya da devam etmektedir. Bunun aksini düşündürecek çalışmalarda vardır. Örnek olarak;

- Tüm işlemlerini sanal ortamlarda yapan kurum ve şirketlerin de sayıları hızla yükselmektedir.
- Bulut ortamlarının diğer ortamlardan daha güvenli olduğunu kabul edenlerin sayısı hızla artmaktadır.
- Ülkeler ve kurumlar bulutun artık güvenli olduğu yönünde hem fikir olmaya başlamışlardır.
- Bulut güvenliği, sanallaştırma güvenliği ve sunucu güvenliği gibi kavramlar hala tartışılmakta ve yeni çözümler geliştirilmeye çalışılsa da kullanımın yaygınlaşması artık bu ortamlara güvenin arttığını da göstermektedir.

Dünya bulut ortamlarında çalışıyor, üretiyor, öğreniyor, yönetiyor, araştırma yapıyor, geliştiriyor, hizmet veriyor, haberleşiyor ve paylaşıyor. Artık sadece insanlar değil makinelerinde elektronik ortamlara dahil edilmesi konuşuluyor. 2020 yılı sonuna tam 50 milyara yakın makinenin bulut ortamına bağlanacağı tahmin ediliyor. Siemens, General Electric gibi şirketler, bilgisayarlarını akıllı hale getirmek ve verimli şekilde kullanabilmek için çalışıyor.

Ülkemize baktığımızda ise bizlerin hala bulut ortamların güvenliğini tartışmaya devam ettiği görülüyor. Bu teknolojileri ülkemizde üreten ve yaygınlaştıran şirketlerin de varlığını ve çabalarını da takdir ettiğimi belirtmek isterim. DivvyDrive ürünü de bunlardan sadece birisidir.

Gelecekte, bu ortamlar ile bunların güvenliği üzerinde daha titizlikle durulacağı muhakkaktır. Burada üzerinde durulması gereken önemli hususlar; bu ortamlardaki risklerin bilinmesi, nasıl azaltıla-

bileceğinin farkında olunması, karşılaşılan tehditleri nasıl giderileceğinin bilinmesi, bilgilerimizi nasıl daha etkin kullanabiliriz gibi hususlara odaklanılması, ve güvenliği yüksek yeni ortamların geliştirilmesidir.

1.7.6. Dijital İkiz (Digital Twin)

Dijital ikiz fikrinin, Avrupa ve Amerika teknolojilerini bir araya getirmek için yapılan çalışmalar neticesinde ortaya çıktığı bilinmektedir. Bu yenilikçi bakış açısı, Amerikan bulut teknolojileri şirketleri ile Avrupa otomasyon teknolojileri şirketlerinin bir araya getirmiş ve sonuçta yeniliklere, endüstriyel veya teknolojik gelişmelere hız kazandırmıştır. Tanım olarak bakıldığında dijital ikiz;

- "gerçek dünya uygulamaları ile sanal dünya çalışmalarını bir araya getirme yaklaşımı",
- "daha anlamlı, gerçekçi, eşzamanlı ve faydalı sonuçlar elde edilmesinde faydalanılan bir çözüm",
- "gerçek-sanal dünya birlikteliğini sağlama yöntemi",
- "fiziksel sistemlere alternatif olarak bunların dijital modellerini geliştirme süreçleri" ve
- "teknolojilerden daha gerçekçi, hızlı ve anlamlı olarak faydalanmada son nokta"

olarak ifade edilmektedir.

Dijital ikiz kavramı içerisinde; insan, sistem, senkronizasyon, gerçek zamanlı çözüm, işletme, süreç, simülasyon, model, analiz, kontrol, denetim gibi pek çok yaklaşımı barındırmaktadır. Diğer bir ifade ile, gerçek dünya problemlerinin daha ayrıntılı ve senkronize olarak dijital ortamda temsil edilebilmesidir.

Bu kavramın daha iyi anlaşılması ve katkısının değerlendirilmesi için literatürden bazı önemli başlıklar ve örnekler aşağıda verilmiştir. Bunlar;

- Gerçek bir uçak motorunun dijital modelinin gerçekçi olarak oluşturulması ve modellenmesidir.
- General Electric, önümüzdeki 20 yıl içinde elektrik talebinin yüzde 50 büyüyeceğini öngörüyor.
- Gartner, bir kaç yıl içerisinde milyarlarca nesnenin aynı zamanda bir dijital ikizi olacağını belirtiyor.

- Siemens, şimdiden pek çok ürününün dijital ikizlerini geliştirmiş durumdadır.
- Ülkemizde dijital ikize verilebilecek ilk örnek GAMA tarafından geliştirilen "İç Anadolu Kombine Çevrim Santralidir."
- Siber güvenlik konusu dijital ikiz üzerinde çalışılan önemli konu başlıklarındandır. Modellenebilen her türlü saldırı, sistem, teknoloji, çözüm, önlem veya yapının dijital ikiz ile kontrol edilebileceği, karşılaşılan olumsuzlukların giderilebileceği, yapılan çalışmaların güvenliğinin artırılabileceği, güvensiz yapı ve organların tespit edilebileceği ve zamanında önlem alınabileceği, kayıpların veya ortaya çıkacak olumsuzlukların ortadan kaldırılabileceği, bir sistemin her parçasının test edilebileceği, bir sorunun kaynağının zamanından önce belirlenebileceği veya denetlenebileceği, sorunun nereden kaynaklandığının öğrenilebileceği, oluşabilecek arıza veya hataların önceden belirlenebileceği gibi pek çok üstünlüğü de bizlere sunabileceği değerlendirilmektedir.

Kısaca açıklayacak olursak; dijital bir ikizin üstünlüklerinden faydalanmak, siber güvenlik çözümleri içinde geçerlidir. Örnek olarak;

- fiziksel bir sistemin dijital bir ikizi ile güvenlik testlerinin daha gerçekçi olarak yapılabilmesi,
- zamanında iyileştirme veya düzeltmelerin tasarımda yapılması ve tamamlanması,
- oluşabilecek ihlallerin önceden belirlenmesi,
- düşük maliyetli çözümler geliştirilmesi,
- zaman tasarrufu sağlanması,
- oluşabilecek sorunların önceden bilinmesi ve
- risklerin önceden belirlenmesi

gibi hususlarda katkılar sağlayacaktır. Ayrıca; dijital bir ikizle sistemi çökerten yinelemeli düzeltmelere gerek kalmayacağı, sorunları doğru bir şekilde belirleme ve çözmenin kolaylaşacağı, ürün eklemelerin kolaylaşacağı, güncellemelerin azalacağı, dijital çağın sunduğu özelliklerden maksimum yararlanılabileceği değerlendirilmektedir.

1.7.7. Kuantum Çözümler

Bu kitabın 2, 4. ve 5. Bölümlerinde bu hususlar detaylı açıklandığından dolayı burada kısaca açıklama yapılacaktır.

Kuantum; üzerinde uzun yıllardır çalışılan konuların başındadır. Buna büyük önem veren IBM, geleceğin en önemli teknolojileri arasında gösterilen kuantum bilgisayarı geliştirmiş, 2016'da 5 qubitlik bir altyapı kurarak bu hizmeti bulut tabanlı olarak araştırmacıların kullanımına sunmuştur. IBM, hem bu bilgisayarı daha da geliştirmiş hem de 50 qubitlik ortamları ticari ortamlara sunmuştur. Bu yılın başında CES 2019'da 20 qubitlik yeni kuantum bilgisayarı tanıtmıştır. System Q One Projesi kapsamında geliştirilen ve ilk kez laboratuvar dışında kullanmak için tasarlanan bu sistem, mevcut sistemler ile entegre olabilecektir. Geliştirme aşamasında olan bu teknolojinin daha tam geliştirilmeden ve kullanıma açılmadan tehditleri olduğu da "kuantum teknolojisi ve yapay zeka gelecek için tehdit" isimli ABD İstihbarat Topluluğu Raporunda 2018 yılı sonunda yayımlanmıştır. Raporda; kuantum teknolojisinin ulusal güvenlik için yeni bir tehdit olduğu, bu teknoloji ile haberleşme sistemlerinin kolayca deşifre edileceği, önlem almanın zor olacağı, ilk hedeflerin ise ABD hükümeti ve askeri operasyonları olacağı belirtilmiştir. Ayrıca raporda; şifreleme sistemleri, otonom ve insansız araçlar ve teknolojilerine zarar vereceği öngörüldüğünden, en üst düzeyde endişe edilen teknoloji listesine alınmıştır.

Genel olarak değerlendirdiğimizde ise gelecek için önemli teknolojik gelişmelerin önünü açacak olan kuantum hesaplama teknolojilerinin; sektörün ve kurumların gelişmesine büyük katkı sağlayacağı fakat beraberinde de büyük endişeleri ve korkuları getireceği de muhakkaktır. Dolayısıyla, geliştirilen bu teknolojilerin siber güvenliğe ve savunmaya bakış açımızı kökten değiştirebilecek yaklaşımlar içerisinde olacağı hem daha hızlı, kaliteli ve güvenli sistemlerin ve uygulamaların geliştirilmesi hem de mevcut sistemlerin tehdit ve tehlike altında kalacağı unutulmadan çalışmalar yürütülmelidir.

1.7.8. Beyin Korsanlığı

Mevcut teoriler ile akademik bilgi birikimi, gelişen teknolojiler ve altyapılar, devam eden çalışmalar, sunulan uygulamalar, yapılan tartışmalar, gelecek öngörüler, sahip olunan yetenek ve gelecekte

hayata geçirilmesi düşünülen projeler değerlendirildiğinde; Düşüncelerimiz öğrenilebilir mi? Beyin veya düşünce korsanlığı mümkün mü?" gibi sorular takılıyor insanın aklına. Peki bu mümkün müdür?

Beyin Korsanlığı (brain hacking) son yıllarda üzerinde tartışılan ve araştırma yapılan önemli konulardan olup, tanım olarak nörobilim, davranış psikolojisi ve sosyoloji gibi alanların sağladığı bakış açılarından faydalanılarak bireyin zihinsel durumunu, bilişsel süreçlerini veya işlev seviyesini etkilemek için teknikler, teknolojiler, yöntemler ve yaklaşımlar kullanılarak yapılan saldırılara verilen isimdir. Bu tür çabaların amacı; her ne kadar, kişisel gelişime katkı sağlama, bilişsel işlevi geliştirme, etkinlik ve mutluluğu optimize etme gibi sağlık tabanlı sebeplere dayandırılsa da aslında amacın bireysel davranışları etkileme, pazarlamayı veya satışları artırma, bireyin zafiyetlerinden ve zayıflıklarından faydalanmaya yöneliktir. Zihin okuma, algı yönetimi vb. konularda bu başlık altında yer almaktadır.

İnsanın nasıl düşündüğünü, davrandığını veya hareket ettiğini anlama ve bunu algoritmik hale dönüştürme çalışmaları, 1950'li yıllardan günümüze artarak devam etmektedir. Temel amaç; beynin muhteşem özelliklerini kullanarak karşılaşılan problemleri zekice çözecek yaklaşımlar geliştirmektir. Günümüzde bu çalışmalar daha kapsamlı hale gelmiş, boyut değiştirmiş, yeni çözümler geliştirilmesinin önünü açmış, yeni bakış açıları kazanmamıza yardımcı olmuş ve yeni hedeflere bizleri odaklamıştır. Bazı örnekler aşağıda verilmiştir.

- Elon Musk'ın "insan beynini bilgisayara bağlamayı" hedeflediği Neuralink Girişim Projesi,
- MIT Üniversitesinin "Yapay Zekadan" "Yapay Genel Zekaya" geçiş çalışmaları,
- Google, Facebook, Twitter vb. şirketlerin geliştirdikleri akıl almaz uygulamalar,
- Büyük veri analitiği ile sadece kişilerin değil toplumsal davranışların, hareketlerin, düşüncelerin analiz edilmesi ve modellenmesi,
- Stanford Üniversitesinde yapılan fare beyninin uzaktan kontrolü çalışması,

- Google'ın Domuz Gribi Projesi,
- IBM'in insanlarla konuşup argümanlar üretmek için tasarladığı yapay zeka tabanlı bilgisayarı (Project Debater),
- Cambridge Üniversitesinin "Gözlerden Zihin Okuma Testi" adını verdiği bir "bilişsel empati" testi,
- UCLA ve Caltech'de yürütülen düşünce ile bilgisayar faresi imlecinin kontrolü projeleri,
- Philips'in düşünce ile ev aletlerini kontrol etme projesi,
- Bilgisayarların insanları, hayvanları ve cisimleri nasıl düşündüğü, anladığı ve tanımladığını anlamaya çalışan Google Deep Dream ve Resimlerden Hikâyeler Üretme projeleri,
- 2200 TED Konuşmasından öğrenerek konuşma yapabilen yapay zekâ sistemi (Machine Generated Talks),
- SAMIM.IO Yapay Zekâ Sistemi,
- Her kullanıcının ayrı iletişim biçimini ve düşünme şeklini taklit etmeye çalışan kişisel robotlar (Örnek: POI.BOT)
- MindRider: Duygusal Durum Ölçme uygulaması,
- Stanford Üniversitesinden Psikolog Prof. Dr. Michal Kosinski'nin yapay zekâ yaklaşımları ile kişilerin cinsel tercihlerini, politik görüşlerini, duygu durumlarını, karakterini, kişisel özelliklerini sadece yüz resimlerinden algılanabileceği ile ilgili çalışmaları ve açıklamaları ve
- AB'de başlatılan "Brain Initiative", "Human Brain Project", "Brain-Machine Interface" vb. proje çalışmalarıdır.

Yukarıda verilen örneklerden, bilgiler, bulgular, projeler, uygulamalar ve açıklamalar beraberinde yeni pek çok soruyu da aklımıza getirmektedir. Genel olarak bakıldığında; teknolojik gelişmeler bizleri büyülemekte, hayatımızı kolaylaştırmakta ve bizlere pek çok yenilik sunmaktadır. Fakat, bunlar yeni korkuları ve tehditleri de beraberinde getirmektedir. Beyin ve zihin korsanlığı, beyni ele geçirme veya kontrol altına alma, zihin okuma, yüz okuma, duygu ve his algılama, algı yönetimi gibi hususlar değerlendirildiğinde, aslında beynimiz büyük bir tehdit altındadır. İsterseniz; Tristan Harris, Michal Kosinski veya Yuval Noah Harari'nin bu konuyla ilgili yaptıkları konuşmaları internetten bulup izleyiniz. Beynimiz heklenir mi? sorusuna cevabı kolaylıkla bulabilirsiniz.

Son olarak; verilerimizi korumaya gösterdiğimiz hassasiyeti beyinlerimize veya zihinlerimize yapılan saldırılara karşı koymak içinde göstermeliyiz. Geleceğimizin teminatı olan beyinlerimizi ve dolayısıyla kendimizi korumak için de göstermek zorundayız.

1.8. Değerlendirmeler

Siber güvenlik ve savunma, mevcut bilgi birikimi, yetenek, kapasite, altyapı, teknoloji, mevcut yöntemler, nitelikli insan kaynağı gibi pek çok konuyu içerisine almaktadır. Bu konudaki değerlendirmelerim ve önerilerim aşağıda maddeler halinde verilmiştir. Bunlar;

- Yüksek seviyede bir koruma için bu bölümde yer verilmeye çalışılan hususlar kapsamlı olarak değerlendirilmeli, gerekli önlemler alınmalı, gelecek projeksiyonlar dikkate alınarak çözümler geliştirilmeli, yatırımlar yapılmalı, ve yeni stratejiler belirlenerek hayata geçirilmelidir.
- Ulusların, kurumların veya toplumların kendi siber güvenliğini sağlamaya yönelik olarak planlama, uygulama, denetleme, önlem alma, koordinasyon ve işbirliği, caydırıcılık gibi konularda etkin olmaları için daha çok çaba harcanmalıdır.
- Ulusal güvenlik için tatbikat yapmak artık bir zorunluluktur. Daha çok yapılmalı ve elde edilen deneyimler paylaşılmalıdır.
- Kümelenme çalışmalarına hız verilmeli ve sağlıklı bir ekosistem kurulmalıdır.
- Kişisel, kurumsal ve ulusal siber güvenliğin sağlanması için yerli ve milli çözümler geliştirilmeli, bütüncül çözümler dikkate alınmalı ve yeni fikir, metot, yöntem, yaklaşım, proje ve ürün geliştirmelidir.
- Yeni nesil problemlerin zeki ve otomatize olacağı dikkate alınarak, yeni ve karşı çözümler geliştirilmelidir.
- Ötesi için güçlerin birleştirilmesi, kaynakların verimli kullanılması, işbirliklerinin artırılması ve belirlenen hedefe doğru odaklanılması gereklidir.
- Ulusal strateji ve eylem planında belirtilen siber güvenlik ekosisteminin geliştirilmesi çalışmaları devam etse de güçlü bir ekosistem oluşturulması ancak ve ancak yerli ve milli teknolojilerin geliştirilmesi, nitelikli insan gücünün yetiştirilmesi, ar-ge ve test

merkezlerinin kurulması, yapılan saldırıların analiz edilmesi ve karşı tedbirlerin geliştirilmesi, siber savunma görev güçlerinin oluşturulması, proaktif önlem alınması, ortak çalışma ortamları belirlenmesi, siber tehdit istihbaratının paylaşılması, karşılaşılan problemlerin çözülmesi için üniversitelerle yapılan ortak çalışmaların artırılması, siber ortam verilerinin anonimleştirilerek araştırmacılara açılması, özellikle zeki gençlerin ilgilerinin bu alana çekilmesi, siber güvenlik ve savunma yetenek havuzlarının oluşturulması, denetim mekanizmalarının daha iyi işletilmesi, standartlaşmanın yaygınlaştırılması, ve en önemlisi siber ekonominin oluşturulması ile olacaktır. Bu kaynakların da yeni ar-ge ve inovasyon çalışmalarında kullanılması çok önem arz etmektedir.

- Kullanıcıların, kişisel verilerini koruyabilmeleri için daha fazla bilgi birikimine, yeteneğine ve yüksek farkındalığa sahip olmalarına gerek vardır. Bunu yapmak zor olsa da mutlaka çaba sarf edilmesi ve konuya daha fazla önem verilmesi gerekmektedir. Kullanıcıların, güvenliği daha basit öğrenebilmeleri, uygulamaları kolayca yönetebilmeleri için kurum ve kuruluşların basit ve hızlı çözümler geliştirmeleri kaçınılmazdır.

- Geleceğimizin daha iyi, mutlu, başarılı ve güvenli olması için, kişisel, kurumsal ve ulusal bilgi güvenliğimizi gözden geçirmeli, eksikliklerin ve aksaklıkların giderilmeli, sorumluluklarımızın farkında olmalı, tehditleri daha yakın takip etmeli ve en önlemlisi ise yeni nesil tehditlere karşı ortak çözümler geliştirmeli, karşılaşılan veya karşılaşılabilecek olumsuzlukların yaşanmaması için "ulusal siber güvenlik yaşam döngüsü" oluşturulmalıdır.
- Sistemlerin, süreçlerin, modellerin, algoritmaların, çözümlerin ve yaklaşımların zekileşmesi, hayatımızda pek çok şeyi değiştirecektir. Bundan mutlaka faydalanılmalıdır. Kısaca ifade etmek gerekirse, "yapay zekâ gelecektir!" ifadesi unutulmadan çalışmalara hız verilmelidir.

Kaynaklar

Bu kitap bölümü, Prof. Dr. Şeref Sağıroğlu'nun aylık olarak CyberMag dergisinde 2018-2019 yılları içerisinde "Editörden" başlığı altında yer alan yazılardan derlenmiş ve genişletilerek burada sunulmuştur.

Siber Güvenlikte Kriptografi

BÖLÜM 2

Doç. Dr. Murat CENK

SİBER GÜVENLİKTE KRİPTOGRAFİ

Bu bölümde, siber güvenlikte kriptografinin rolü üzerinde durulmaktadır. Özellikle veri saklama ve haberleşmede bilinen saldırılara karşı kriptografik teknikler ile güvenliğin nasıl sağlandığı sunulmakta ve bu konunun güncel durumu açıklanmaktadır. Ayrıca, sistemlerin güvenliklerini sağlayabilmek için kullanılan kriptografik teknikler hakkında bilgi verilmektedir.

2.1. Giriş

Günümüzde yüksek kapasiteli bilgisayarlar, mobil cihazlar ve bulut sistemler gibi teknolojiler kullanılarak dijital verilerin saklanması ve bunların iletilmesi çok kolay hale gelmiştir. Milyonlarca kişi ve makine birbirleriyle internet üzerinde haberleşmekte ve verilerini sunucularda saklamaktadırlar. Örneğin, bir seyahat için bilet alırken birçok satıcıyı internet üzerinden kolayca araştırıp bize en uygun olanını kredi kartımızı kullanarak alabilmekteyiz veya tüm dijital dosyalarımızı bulut sistemlere yükleyip internet bağlantısının olduğu her yerden bu dosyalara kolayca ulaşabilmekteyiz. Yaşantımızı kolaylaştırarak milyarlarca dolar ekonomik katkı sağlayan bu ve benzeri sistemler ancak ve ancak güvenli olduğu takdirde kullanışlıdır. Mesela, yukarıda bahsedilen güvenli olmayan bir sistemden bilet alırken kullandığımız kredi kartı bilgileri veya bulut sisteme yüklediğimiz kişisel bilgiler kolaylıkla istenmeyen kişilerin eline geçebilmektedir. Bahsedilen ve benzeri sistemlerin güvenliklerini sağlamak için kriptografik teknikler yaygın olarak kullanılmaktadır. Kriptografi, bir verinin içeriğinin anlaşılmayacak şekilde değiştirilmesi ve sadece gizli anahtar kullanarak makul bir zamanda tekrar eski haline getirilmesidir. Bu işlemler, ileri düzey matematik teknikler kullanılarak yapılmaktadır ve böylece siber sistemlerde olması gereken gizlilik, kimlik doğrulama, veri bütünlüğü ve inkâr edememezlik gibi güvenlik gereksinimleri sağlanmaktadır.

Bu bölümün amacı, siber sistemlerin güvenliklerini sağlamada kriptografinin nasıl kullanıldığını ve bu alandaki güncel konular hakkında gelişmeleri vermektir. Bir sonraki bölümde saldırı çeşitleri sunulacak ve güvenli olmayan sistemlerde bilgilerin nasıl ele geçirildiği bahsedilecektir. Sonra, kriptografi ile ilgili temel tanımlar ve çeşitleri sunulacaktır. Kriptografi kullanılarak internet güvenliği, kablosuz ağ güvenliği, bulut güvenliği, nesnelerin interneti güvenliği ve parola güvenliği verildikten sonra, son olarak kriptografiye büyük etkileri olan kuantum bilgisayarlar ve kuantum sonrası kriptografi üzerine güncel gelişmeler sunulacaktır.

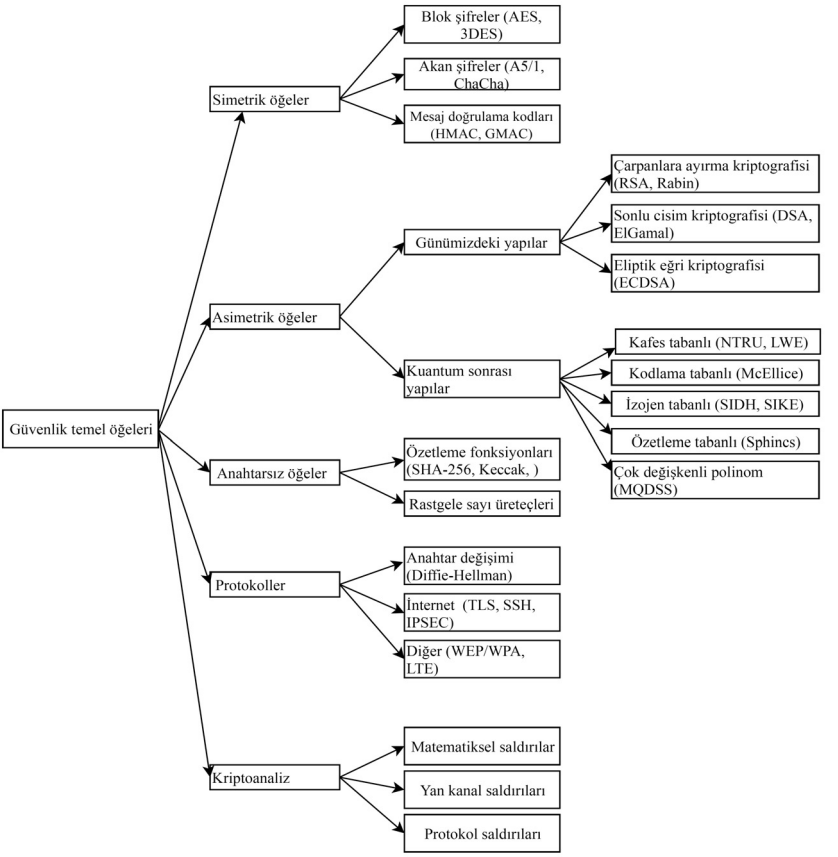
2.2. Saldırı Örnekleri ve Güvenlik Kavramları

Siber sistemler kullanılarak yapılan haberleşmede veya bilgi depolamada güvenlik tedbirleri alınmamışsa saldırganlar kolaylıkla bu bilgileri elde edebilir. Güvenlik tedbirleri alınmamış bir haberleşme sisteminde saldırganlar gönderilen mesajları dinleyebilir, değiştirebilir, başkasının adına mesaj gönderebilir veya gönderilen mesajı elde ederek başka bir zaman bu mesajı kullanabilir. Ağda yapılan bu tür saldırılara ortadaki adam saldırıları denmektedir. Diğer taraftan özel veya gizli bir bilgiyi depolarken güvenlik tedbirleri alınmamış bir sistemden bu bilgiler istenmeyen kişiler tarafından elde edilebilir veya değiştirilebilir. Örneğin, bu bilgi sistemdeki kullanıcıların parola bilgileri olduğunda durumun ne kadar ciddi olduğu kolaylıkla görülebilir. Bu tür istenmeyen durumların olmaması için sistemlerde gizlilik, bütünlük, kimlik doğrulama ve inkâr edememezlik şartları sağlanmalıdır. Gizlilik, bir bilginin yetkisiz kişilerin eline geçse dahi içeriğinin o kişilerce elde edilememesi; bütünlük, verinin içeriğinin değiştirildiğinde anlaşılması; kimlik doğrulama, göndericinin kimliğinin doğrulanması ve inkâr edememe ise, gönderen kişinin daha sonra gönderdiği mesajı inkâr edememesi olarak tanımlanabilir. Güvenli bir sistemde zafiyet olmaması için bu şartların hepsinin sağlanması gerekir. Bu gereksinimleri sağlayabilmek için de kriptografik teknikler kullanılmaktadır.

2.3. Kriptoloji Bilimi

Şifreleme bilimi olarak bilinen kriptoloji başlıca kriptografi ve kriptoanaliz olarak iki bölüme ayrılmaktadır. Bu bölümde bu kavramlar ve bunların alt alanları ile kriptolojide oldukça önemli bir yer tutan

kriptografik özetleme fonksiyonları sunulmaktadır. Güvenlik temel öğelerinin sınıflandırılması Şekil 2.1'de verilmiştir.



Şekil 2.1. Güvenlik temel öğelerinin sınıflandırılması

2.3.1. Kriptografi

Kriptografi, bir veriyi iletirken veya depolarken bir anahtar ve fonksiyon kullanarak bu verinin anlaşılmayacak bir hale getirilmesi (şifreleme) ve istenildiği zaman bir anahtar ve fonksiyon yardımı ile orijinal haline dönüştürülmesi (deşifreleme) olarak tanımlanabilir. Kriptografi, simetrik kriptografi ve asimetrik kriptografi (açık anahtarlı kriptografi) olarak ikiye ayrılır. Simetrik sistemlerde, şifreleme ve deşifrelemede aynı anahtar veya birbirinden kolaylıkla elde edilebilen gizli bir anahtar kullanılırken; açık anahtarlı kriptografide, her kullanıcının açık ve gizli olmak üzere iki anahtarı vardır.

2.3.1.1. Simetrik Kriptografi

Simetrik kriptografi, genellikle gizliliğin sağlanmasında kullanılmaktadır ve simetrik sistemler oldukça verimli sistemler olup blok şifreler ve akan şifreler olarak ikiye ayrılır. Blok şifrelerde anahtar boyutu genellikle 128, 192 veya 256 bit boyutlarında olup iletilmek istenen mesaj bu uzunluklara bölünüp şifreleme yapılır. Akan şifrelerde ise anahtar boyutu iletilmek istenen mesajın uzunluğuna eşit olup şifreleme, genellikle mesaj bitlerinin anahtar bitleri ile XOR işlemi yapılarak elde edilir. Pratikte mesaj boyutu uzunluğunda anahtar üretilip dağıtılması kolay değildir. Bundan dolayı akan şifrelerde anahtar dizisi adı verilen sözde rastgele sayı bitleri üretilir ve bu bitler mesaj bitleri ile işleme alınır. Burada haberleşmek isteyen tarafların ortak anahtar dizisini üretmek için daha küçük boylu gizli bir anahtar paylaşmaları gerekmektedir. Blok şifrelere örnek olarak 3DES, AES ve SERPENT gibi algoritmalar verilebilir [1]. Diğer taraftan A5/1, A5/2, RC4, Salsa20 ve ChaCha gibi algoritmalar ise akan şifrelere örnektir [2]. Gönderici ve alıcı genellikle aynı anahtarı kullandıkları için haberleşmek isteyen her iki taraf aynı anahtara sahip olmak zorundadır. Bir ağda n kişi varsa, toplam $n(n-1)/2$ farklı anahtar oluşturulması gerekmektedir. Bundan dolayı, anahtarların oluşturulması ve güvenli bir kanalla dağıtılması sorun teşkil etmektedir. Ayrıca kullanılan anahtar tek bir kişide olmadığı için inkâr edememezlik gereksinimi bu sistemler ile sağlanamamaktadır.

2.3.1.2. Asimetrik Kriptografi

Anahtar dağıtımı ve inkâr edememezlik gibi gereksinimler asimetrik kriptografi ile çözülebilmektedir [3]. Bu tip kriptografi aynı zamanda açık anahtarlı kriptografi olarak adlandırılmaktadır. Mesaj gönderilmek istenen kişinin herkes tarafından bilinen açık anahtarı, gönderici tarafından şifrelemede kullanılarak gizlilik sağlanırken, kullanıcı kendi gizli anahtarını kullanarak kimlik doğrulama ve inkâr edememezlik gereksinimlerini sağlayabilmektedir. Şu anda gerçek hayat uygulamalarında kullanılan açık anahtar kriptografi başlıca üç gruba ayrılır. Bunlar çarpanlara ayırma kriptografi, sonlu cisim kriptografi ve eliptik eğri kriptografi olarak adlandırılır. Çarpanlara ayırma kriptografisine örnek olarak RSA, sonlu cisim kriptografisine örnek olarak ElGamal ve DSA, eliptik eğri kriptografisine örnek olarak ECDSA algoritmaları verilebilir. Bunların dı-

şında da birçok açık anahtar sistemi vardır. Bunların başlıcaları, çok değişkenli ikinci derece polinom kriptografi, kafes tabanlı kriptografi, kod tabanlı kriptografi, özet fonksiyon tabanlı kriptografi ve süper tekil izojen tabanlı kriptografidir. Son yıllara kadar özellikle verimlilik yönünden avantajlı olmadıkları için pek kullanılmayan bu sistemler kuantum bilgisayarların şu anda kullanılan çarpanlara ayırma kriptografiyi, sonlu cisim kriptografiyi ve eliptik eğri kriptografiyi güvensiz hale getirmesinden dolayı tercih edilmeye başlanmıştır ve bu sistemler kullanılarak yeni birçok sistem geliştirilmiştir. Ayrıca, Amerika Birleşik Devletleri'nin Ulusal Teknoloji Standart Kurumu (NIST) hem klasik bilgisayarlar hem kuantum bilgisayarlar ile yapılan saldırılara karşı dayanıklı yeni açık anahtar kripto sistemleri seçme süreci başlatmıştır [4] ve bundan dolayı kuantum sonrası kriptografiye olan ilgi artmıştır. Bu makalenin son bölümü bu konuya ayrılmıştır.

2.3.1.3. Kriptografik Protokoller

Kriptografik protokoller bilgiyi güvenli hale getirmek için kriptografik algoritmalar kullanılanarak kurallar oluşturma olarak tanımlanabilir. Kriptografik protokollerin başlıca kullanım yerleri anahtar anlaşmaları, kimlik doğrulama, inkâr edememe, sır paylaşımları, veri bütünlüğü ve güvenli çok katılımlı hesaplamalardır. Bunların dışında elektronik veya internet oylama, zaman damgası, dijital paralar gibi daha ileri düzeyde kriptografik protokoller de vardır. İnternet güvenliğini sağlayan SSL/TLS protokolü bu makalenin internet güvenliği bölümünde açıklanmıştır.

2.3.2. Kriptoanaliz

Kriptografik algoritmaların güvenliğini inceleyen bilim dalına kriptoanaliz denmektedir. Bu alan, kriptografik algoritmalar ile elde edilmiş şifrelenmiş metinlerden orijinal metin elde etmeye veya gizli anahtarı elde etmeye çalışarak bu algoritmaların güvenliklerini inceler. Kriptoanaliz yaparken elimizde açık mesaj ve buna karşılık gelen şifreli mesaj varsa buna bilinen açık mesaj saldırısı (known plaintext attack), sadece şifreli metin varsa, sadece şifreli metin saldırısı (ciphertext only attack), elimizde bir şifreleme cihazı var ve biz istediğimiz metni şifreleyebiliyorsak buna seçilen açık mesaj saldırısı (chosen plaintext attack) ve elimizde bir deşifreleme cihazı

varsa ve istediğimiz metni deşifreleyebiliyorsak bu atağa da seçilen şifreli metin saldırısı (chosen ciphertext attack) denir. Kriptoanaliz konusu, matematiksel kriptoanaliz, yan kanal saldırıları ve protokol saldırıları olarak başlıca üç grup altında toparlanabilir.

2.3.2.1. Matematiksel Kriptoanaliz

Bu yaklaşım matematiksel metotlar ile gizli anahtarı elde etmeye çalışmaktadır. Örnek olarak RSA açık anahtarlı kriptografide, gizli anahtarı açık anahtardan elde etmek için herkes tarafından bilinen ve iki büyük asal sayının çarpımından oluşan n sayısını çarpanlara ayırmaya çalışmak verilebilir. Literatürde kaba kuvvet saldırısından çok daha hızlı çalışan birçok çarpanlara ayırma algoritması vardır. Mesela eliptik eğri çarpanlara ayırma metodu buna bir örnektir. Bir kripto sistem için güvenli anahtar uzunluğu belirlenirken, bu anahtar uzunluğu kullanıldığı durum için sistemin bilinen tüm ataklara karşı dayanıklı olması test edilir. Örneğin RSA ile 112 bitlik bir güvenlik seviyesi sağlayabilmek için anahtar boyu 2048 bit olarak seçilmek zorundadır. Bu durumda literatürdeki en hızlı çarpanlara ayırma algoritması olan sayı alan eleği (number field sieve) algoritması ile yapılan saldırının çalışma süresi 2^{112} adım sürecektir.

2.3.2.2. Yan Kanal Atakları

Yan kanal atakları sistemin gerçekleştirilmesi aşamasındaki yapılan zayıflıkları kullanarak gizli anahtarı elde eder. Bu saldırı çeşidinde kriptografik bir algoritmanın çalışma zamanı veya güç tüketimi gibi bilgiler kullanılır. Örneğin, RSA algoritmasında şifreleme yaparken kullanılan modüler üst alma yönteminde kullanılan kare al ve çarp metodu gerçekleştirilirken dikkat edilmemişse, gizli anahtarın bitlerinin 1 olduğu yerde daha çok zaman ve güç gereksinimi olacağından saldırgan gizli anahtarı kolaylıkla elde edecektir. Bundan dolayı kriptografik sistemlerin gerçekleştirilmesinde kullanılan algoritmalar dikkatlice seçilmeli ve yan kanal ataklarına karşı önlem alınarak gerçekleştirilmelidir. Bu amaçla yapılan karşı önlemlerden bir tanesi kriptografik algoritmaları sabit zamanlı gerçekleştirmektir. Böylece, kriptografik algoritmalar anahtardan bağımsız olarak sabit zamanlı çalışır ve anahtar ile ilgili bir bilgi ortaya çıkmaz. Sabit zamanlı gerçekleştirme yapmak çok dikkat gerektiren bir husus olup bu konuda bir çok öneri vardır. Bu tür gerçekleştimeleri zorlaştıran

etkenlerden bir tanesine "if" komutunun kullanılması örnek olarak verilebilir. Yazılım sürecinde anahtardan bilgi alarak işlem yapılan yerlerde "if" komutu yerine alternatif komutlar kullanılması sabit zamanlı bir gerçekleştirme yapılmasına katkıda bulunur.

2.3.2.3. Protokol Atakları

Protokol atakları kriptografik algoritmaların zayıflıklarından ziyade protokol tasarımında bulunan zayıflıkların kullanılarak gizli bilginin ele geçirilmesidir. Örnek olarak, Diffie-Hellman anahtar değişiminde ortadaki adam saldırısı verilebilir. Bu protokolde p bir asal sayı ve g ise p elemanlı sonlu cismin bir üreteci olup bunlar sistemin açık parametreleridir. A ve B ortak anahtar üretirken A, a rastgele sayısını ve B ise b rastgele sayısını seçer. Burada a ve b sayıları 2 ile p-2 arasındadır. Daha sonra A tarafı $g^a \bmod p$ sayısını B tarafı ise $g^b \bmod p$ sayısını hesaplayıp karşı tarafa gönderir. Son aşamada ise, A tarafı, $(g^b)^a \bmod p$ sayısını, B tarafı ise $(g^a)^b \bmod p$ sayısını hesaplar. Artık her iki taraf da ortak anahtar olan $g^{ab} \bmod p$ sayısını elde etmiştir. Bu protokol Şekil 2.2'de verilmiştir.

Açık parametreler: p,g	
A	B
Rastgele a seçilir.	Rastgele b seçilir.
$g^a \bmod p$ hesaplanır.	$g^b \bmod p$ hesaplanır.
$g^a \bmod p \rightarrow$	$\leftarrow g^b \bmod p$
$(g^b)^a \bmod p$ hesaplanır.	$(g^a)^b \bmod p$ hesaplanır.

Şekil 2.2. Diffie-Hellman ortak anahtar oluşturma protokolü

Bu sistemde, ortadaki adam $g^a \bmod p$ ve $g^b \bmod p$ sayılarını elde etse bile ortak anahtar olan $g^{ab} \bmod p$ sayısını elde edebilmesi için burada a ve b sayılarını elde etmesi gerekmektedir. Bu ise matematikte uygun parametreler altında zor olarak bilinen ayrık logaritma problemidir ve bundan dolayı sistem matematiksel olarak güvenlidir. Fakat, sistemin kimlik doğrulaması olmadığından ortadaki adam iletişimi kesip kendi sayılarını A ve B taraflarına göndererek iki farklı ortak anahtar oluşturup tüm haberleşmeyi dinleyebilir. Bu, protokolün zayıflığından kaynaklanan bir saldırıdır ve bu tip saldırılara karşı çok dikkatli olunmalıdır. Bu sisteme kimlik doğrulamayı ekleyerek saldırıya karşı gelinebilir.

2.3.3. Özetleme fonksiyonları

Kriptografide kullanılan önemli bir fonksiyon tipine özetleme fonksiyonu [5] denmektedir. Kriptografik özetleme fonksiyonları pratik uygulamalarda önemli rol oynamaktadır. Özetleme fonksiyonu, girdisi keyfi uzunlukta ama çıktısı sabit uzunlukta (genellikle 256 ve 512 bit gibi küçük boyutlarda) olan fonksiyonlara denmektedir. Bu fonksiyonların kriptografik olarak adlandırılabilmesi için bazı şartları sağlamaları gerekmektedir. Kriptografik özetleme fonksiyonunun öncelikle hesaplanmasının kolay olması gereklidir. Ayrıca, özet değeri verilmiş bir girdinin bulunmasının zor olması gereklidir (tek yön fonksiyon özelliği). Ek olarak sabit bir girdiyle aynı özet değeri olan başka bir girdinin bulunması zor olmalıdır. Son olarak sağlanması en zor olan özellik ise, aynı özet değerine sahip iki farklı girdinin bulunmasının zor olması özelliğidir (Doğum günü paradoksu sebebi ile bu tip çakışmaların bulunması, hesaplama yönünden diğerlerine göre kolaydır). Bu şartlara sahip özetleme fonksiyonlarına kriptografik özetleme fonksiyonları denmektedir. Bu fonksiyonlar kriptografik uygulamalardaki önemli gereksinimlerden olan kimlik doğrulama, elektronik imza algoritmaları, bütünlük ve rastgele sayı üretimi konularında sıklıkla kullanılmaktadır. Ayrıca, son zamanlarda blok zincir teknolojilerinin uygulamalarında da kullanılmaktadır.

Özetleme fonksiyonlarının başlıca iki farklı çeşidi vardır. Bunlar sadece bu iş için adanmış fonksiyonlar ve blok şifre tabanlı fonksiyonlardır. Blok şifre tabanlı özetleme fonksiyonlarında blok şifrelerin rastgele çıktı verme özelliği kullanılmaktadır. Adanmış fonksiyonlar için ise bir çok farklı metot önerilmiştir. Pratikte oldukça kullanılmış fakat şu anda artık kriptografik olarak güvensiz olan MD5 ailesi ve SHA-1 bu tip için bazı örneklerdir. NIST kurumu 2001 yılında SHA-256, SHA-384 ve SHA-512 algoritmalarını 128, 192 ve 256 bit güvenlik seviyesi için önermiştir. Ayrıca 2004 yılında 3DES algoritması ile uyumlu olması için SHA-224 fonksiyonu verilmiştir. Bunların hepsi SHA-2 olarak adlandırılmaktadır. Daha sonra NIST 2008 yılında SHA-3 standartlaşma sürecini başlatmış ve 33 algoritma içinden Keccak algoritması seçilmiştir. Bu algoritma SHA-3 olarak adlandırılmaktadır.

2.4. Kriptografi Temelli Siber Güvenlik

Siber uzay; kullanıcılar, internet, birbirine bağlı bilgisayarlar ve onların ağlarını içeren bir ortam olarak tanımlanabilir. Siber uzay ve buradaki kullanıcıların değerlerini koruyan araçlar ve politikalar ise, siber güvenlik olarak tanımlanabilir. Buradaki en büyük tehlike, bilginin istenmeyen kişilerin eline geçmesidir ve siber güvenlik bunun engellenmesini amaçlar. Siber güvenlik sorunlarının üstesinden gelmek için kimlik doğrulama, şifreleme, sayısal imza, bütünlük, antivirüs yazılımları ve güvenlik duvarları gibi araçlar ve teknikler kullanılmaktadır. Bunlardan şifreleme, kimlik doğrulama, sayısal imzalama ve bütünlük gereksinimleri, kriptografik teknikler ile sağlamaktadır. Bu bölümde, kriptografik tekniklerin internet güvenliği, kablosuz ağ güvenliği, bulut güvenliği, nesnelerin interneti güvenliği ve parola güvenliği gibi seçilmiş bazı önemli konularda nasıl güvenlik sağladığı anlatılmaktadır.

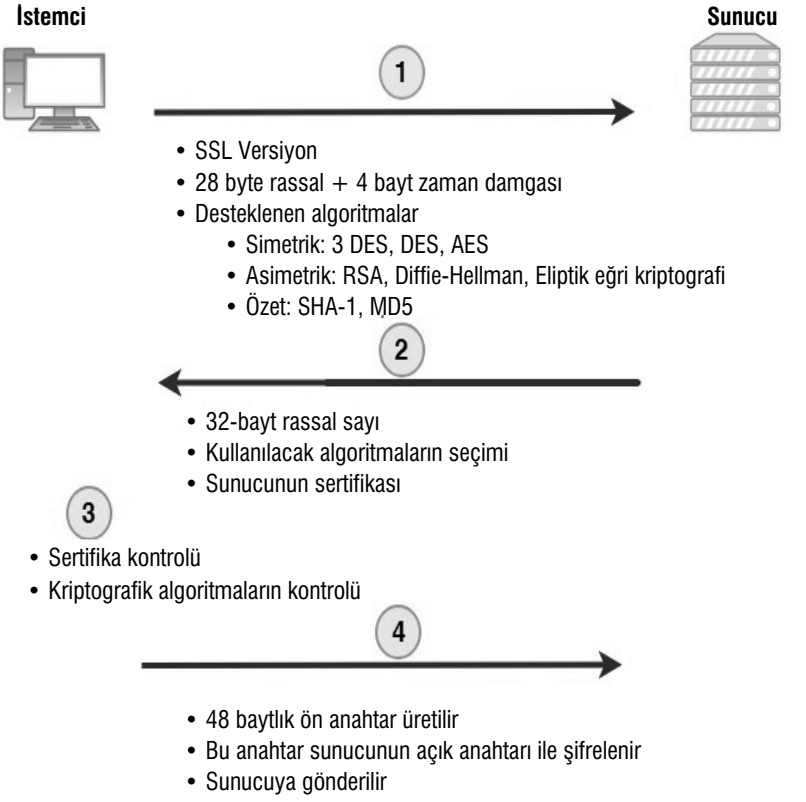
2.4.1. İnternet Güvenliği

Kriptografinin uygulamalarından bir tanesi internet üzerinde güvenli iletişimi sağlamaktır. Bu amaç için SSL (Secure Socket Layer – Güvenli Soket Katmanı) ve TLS (Transport Layer Security – Taşıma Katmanı Güvenliği) protokolleri kullanılmaktadır. SSL protokolü ilk kez 1995 yılında Netscape şirketi tarafından güvenli internet iletişimi için önerilmiştir. SSL protokolünün 3 sürümü yapıldıktan sonra 1999 yılında TLS olarak adlandırılmıştır. SSL ve TLS'in genel olarak birçok özelliği ortaktır. Sadece güvenlik açığı bulunan bazı algoritmalar değiştirilerek yeni sürüm adlandırılmıştır.

SSL/TLS protokolü, başlıca kayıt ve yönetim protokollerinden oluşmaktadır. Kayıt protokolü sıkıştırma ve iki taraf arasındaki verilerin şifrelenmesi ile ilgilidir. Diğer taraftan yönetim protokolü, kayıt protokolünde kullanılan parametrelerin oluşturulmasından sorumludur. Bu bölümün en önemli bileşeni ise el sıkışma protokolüdür. SSL'deki el sıkışma protokolünün basit bir anlatımı Şekil 2.3'te verilmiştir. TLS'deki durum ise SSL ile benzer şekilde çalışmaktadır.

İstemci ve sunucu arasındaki verilerin şifreli olarak iletilmesinde kullanılacak olan oturum anahtarının oluşturulmasını sağlayan el sıkışma protokolünde, öncelikli olarak istemci sunucuya SSL versiyonu, 32 baytlık rastgele bir sayı (Bunun son 4 baytı zaman damga-

sıdır.) ve desteklenen algoritmaları gönderir. Bu algoritmalar, 3DES ve AES gibi blok şifre algoritmaları, RSA, Diffie-Hellman anahtar değişimi ve eliptik eğri kriptografi gibi açık anahtarlı algoritmalar ve SHA-1 veya SHA-256 gibi özet fonksiyon algoritmalarıdır. Bu bilgileri alan sunucu, kullanılacak algoritmaların seçimini, sunucunun sertifikasını ve 32 baytlık rastgele bir sayıyı istemciye gönderir. İstemci daha sonra sertifika kontrolünü yaparak sunucunun kimlik doğrulamasını ve kullanılacak algoritmaların kontrolünü yapar. Bunların doğrulamasından sonra istemci 48 baytlık rastgele bir sayı üretir. Bu anahtar, sunucunun açık anahtarı ile şifrelenerek güvenli bir şekilde sunucuya iletilir. Artık istemcide ve sunucuda gizli olarak üretilmiş ve paylaşılmış olan 48 baytlık bir ön anahtar vardır. Bu ön anahtar bazı özet algoritmalarından geçirilir ve iletişimde kullanılacak olan ortak gizli anahtarlar kolayca oluşturulur.



Şekil 2.3. SSL el sıkışma protokolünün kolay bir gösterimi

2.4.2. Kablosuz Ağ Güvenliği

Kriptografinin kullanıldığı uygulamalardan bir diğeri ise kablosuz ağ güvenliğidir. Kablosuz ağ güvenliğinin en önemli gereksinimleri arasında veri iletiminin gizliliği, iletilen verinin bütünlüğü ve kimlik denetimi vardır. Kablosuz ağ iletişimini korumak için önerilen WEP (Wired Equivalent Privacy) protokolü, şifreleme ve mesaj bütünlüğünü koruyan mekanizmalar kullanmasına rağmen ciddi güvenlik sorunlarına sahiptir. Bu sebeplerden dolayı yeni bir çalışma yapılmıştır ve 2002 yılında WPA (Wi-Fi Protected Access) protokolü önerilmiştir. WEP'deki zayıflıkların geçici olarak çözmeyi amaçlayan WPA'dan sonra 2004 yılında WPA2 çıkarılmıştır. WPA2 veri iletişiminde güvenlik, AES blok algoritmasının şifre blok zincirleme mesaj doğrulama kodu ile birlikte kullanılan sayaç modu (counter mode with cipher block chaining message authentication code) ile sağlanır. WPA2 yerine Ocak 2018 tarihinde WPA3 standardı duyurulmuş ve gizlilik, bütünlük ve kimlik denetimi gibi gereksinimler daha da güvenli hale getirilmiştir.

2.4.3. Bulut Güvenliği

Son yıllarda artarak kullanılmaya başlanan teknolojilerden bir diğeri bulut teknolojisidir. Bulut servisler kullanıcılarına internet bağlantısı olan her yerden ulaşma imkanı veren çok büyük depolama alanları ve yüksek hesaplama gücü sağlamaktadır. Buradaki en önemli gereksinimlerden bir tanesi verilerin gizliliğidir. Bulut sistemlere depolanan verilerin gizliliği kriptografi ile sağlanabilmektedir. Verileri bulutta şifreli tutmak, verilerin istenmeyen kişilerin eline geçmesi halinde bile içeriklerinin gizli kalmasını sağlamaktadır. Ayrıca buluttaki veriler üzerinde hesap yapabilmek için verilerin her defasında deşifrelenip sonra şifrelenmesinden doğan zaman kaybını önleyen homomorfik şifreleme metodu [6] son yıllarda oldukça yoğun bir şekilde çalışılmaktadır ve bu konuda birçok pratik çözüm elde edilmeye başlanmıştır. Bu yaklaşım ile şifrelenmiş olarak tutulan veriler üzerinde toplama veya çarpma işlemleri yapıldığında çıkan sonuç açık mesajların toplama veya çarpılması ile elde edilen sonucun şifreli haline eşittir. Ayrıca kriptografi alanındaki önemli bir araştırma konusu da aranabilir şifrelemedir (searchable encryption). Bu yaklaşım, şifrelenmiş metinler üzerinde arama yapabilme imkanı vermektedir. Homomorfik şifreleme ve aranabilir

şifreleme, bulut sistemlerinin daha güvenli ve kullanışlı olmalarına olanak tanıyan yaklaşımlardır.

2.4.4. Nesnelerin İnterneti Güvenliği

Güvenlik ihtiyacına acilen ihtiyaç duyulan güncel bir konu ise nesnelerin interneti konusudur. Nesnelerin interneti ile günlük hayatımızda kullandığımız cihazların birbirlerine internet üzerinden bağlanarak veri alıp gönderilmesi kastedilmektedir. Sensör teknolojisinin gelişmesi ile birlikte birçok cihaz geliştirilmiş ve akıllı ev veya şehirler gibi kavramlar ortaya çıkmıştır. Böylece hayatımızı kolaylaştıran birçok uygulama yapılmıştır. Örnek olarak, bizler işten eve gelirken evlerimizin belirli bir saatte ısıtılmaya başlanması veya eve varmaya belirli bir mesafe kala fırını çalıştırma komutu verip yemeğin pişmesinin eve vardığımızda bitmiş olması verilebilir. Tahmin edileceği üzere bu cihazlarla internet üzerinden bilgi alışverişi yapılması güvenlik gereksinimlerini ön plana çıkarmaktadır. Buradaki tehditlerin başında cihazların kaynak kısıtlı olmalarından dolayı kimlik doğrulama ve şifreleme gibi güvenlik sağlayan kriptografik mekanizmaların yeteri kadar güvenli olmaması gelir. Güvenliğin önemli olduğu bu sistemlerde standartlarda önerilen algoritmaların kullanılması çok önemlidir. Özellikle, daha çok performans elde etmek için daha önce kullanılmamış veya test edilmemiş algoritmalar kullanılmamalıdır. Literatürde bu tür sistemler için geliştirilmiş hafif sıklet algoritmalar analiz edilmeli ve bunlar dikkatlice ve güvenli bir şekilde sisteme eklenmelidir. Bu konuda yapılan standartlaşma çalışmaları [7] sitesinden incelenebilir.

2.4.5. Parola Güvenliği

Kriptografik teknikler kullanılarak güvenlik sorunlarının çözüldüğü diğer bir konu parola güvenliğidir. Parolalar oldukça yaygın olarak kullanılmaktadır. Artık hemen hemen her internet sitesinde işlem yapabilmek için kullanıcıların o siteye üyeliği ve buna karşılık gelen bir parola oluşturması gerekmektedir. Bu parolalar sunucularda parola dosyasında saklanmaktadır. Eğer bu dosya açık bir şekilde tutulursa, bir saldırgan bu dosyayı ele geçirdiğinde kullanıcıların parolalarını elde etmiş olur. Bu tür zafiyetleri ortadan kaldırmak için kullanıcıların parolalarının tutulduğu dosyadaki bilgiler açık olarak tutulmaz. Genellikle bu bilgiler güvenli bir kriptografik

özetleme fonksiyonundan geçirilerek tutulur. Kriptografik özetleme fonksiyonları tek yönlü ve çakışmaya karşı dayanıklı olduğundan, bu dosyayı ele geçiren bir saldırgan özetleme fonksiyonu sonucundan parolalara erişemez. Fakat, dikkatlice seçilmemiş parolalar halen tehlike altındadır. Sözlük atakları ile saldırganlar parola dosyalarındaki basit seçilmiş parolaları elde edebilmektedir. Bu saldırıda, saldırgan daha önceden oluşturulmuş sözlükteki tüm sözcüklerin özet değerlerini parola dosyası ile karşılaştırır ve sözlükteki kelimeleri parola olarak seçmiş kişilerin parolalarını ele geçirir. Buradaki sözlüğe çok basit olabilecek parolalar ve belirli kelimelerin kombinasyonları da eklenerek sözlük saldırısı ile elde edilebilecek parola sayısı artırılabilir. Burada bu saldırıya karşı alınabilecek önlemlerden bir tanesi sistem yöneticilerinin parola dosyalarını oluştururken özet alma sürecinde tuzlama (salting) adı verilen rastgele seçilmiş belirli uzunluktaki bitlerin parolaya eklenerek özetin alınmasıdır. Bu durumda saldırganın sözlük atağını uygulayabilmesi için eklenen rastgele sayının bit sayısı n olmak üzere 2^n farklı sözlük oluşturması gerekmektedir. Bu ise örneğin n sayısı 10 olduğunda 1024 farklı sözlük oluşturulması anlamına gelmektedir ve pratikte bu atağın uygulanabilirliği zorlaşmaya başlamaktadır. Buradaki n sayısı 20 değerini geçmeye başladıktan sonra bu saldırının pratikte uygulanabilirliği ortadan kalkmaktadır. Bu sebeplerden dolayı güvenliği sağlamak için bu tür yaklaşımlar kullanmak gerekir. Burada bilinmesi gereken konulardan bir tanesi bu tekniğin belirli bir kişinin güvenliğini korumaktan ziyade sistemdeki zayıf parola seçmiş kullanıcıların bilgilerinin saldırganların eline geçmesini zorlaştırmasıdır. Ek olarak, parola dosyalarında özet foksiyonları kullanmak yerine 3DES ve AES gibi blok şifre algoritmaları da kullanılabilir. Ayrıca bu algoritmalar doğru ve güvenli bir şekilde kullanılmalı ve gerçeklenmelidir. Mesela, blok şifrelerin elektronik kod modunda (ECB) kullanılması büyük bir güvenlik açığına sebep olmaktadır. Geçmişte bu durumdan dolayı milyonlarca kullanıcının parolaları saldırganların eline geçmiştir.

Sonuç olarak parola konusu ile ilgili kullanıcıların dikkat etmesi gereken hususlar şöyle sıralanabilir. Öncelikle kullanıcılar her internet sitesi için farklı bir parola seçmelidir. Aksi takdirde tüm üyeliklerde aynı parola kullanılırsa bu durum büyük sorunlara sebep olabilir. Mesela, bir sitenin güvenlik zafiyetinden dolayı parola sal-

dırganların eline geçtiği takdirde kullanıcının diğer sitelerdeki kullandığı parolalar da ele geçirilmiş olur. Bundan dolayı kullanıcılar her hesap için farklı bir parola oluşturmalıdır. Bu parola yukarıda açıklanan sözlük saldırılarına karşı dayanıklı olması için kolayca tahmin edilemeyen ve sözlüklerde kullanılan kelimelerin kombinasyonu olmamalıdır. Karakter sayısı 10 karakter veya daha fazla olmalı ve sayılar da kullanılmalıdır. Ayrıca büyük harf ve "%", "&" veya "!" gibi özel karakterlerin kullanılması güvenliği artırmaktadır. Böyle kurallara uyularak parola üretilmesi ve daha da önemlisi hatırlanması kolay değildir. Üye olunan hesap sayısının her geçen gün arttığını düşünürsek, bu durumun çok zor olduğu söylenebilir. Bu problemi çözmek için parola yönetim programları vardır. Ticari ve açık kaynak kodlu ücretsiz olan uygulamalar kullanıcıların parolalarını şifreli bir şekilde güvenli olarak tutmaktadır. Kullanıcıların sisteme girmeleri için gerekli olan güvenli bir anahtar oluşturmaları ve sadece bunu hatırlamaları yeterlidir. Ana anahtar olarak adlandırılan bu anahtar ile tüm hesapların farklı ve güvenli olarak oluşturulmuş parolaları güvenli bir şekilde şifrelenir ve şifreli olarak saklanırlar. Bu ana anahtar kullanılarak sisteme girildikten sonra tüm parolalara deşifreleme işlemi yapılarak erişim sağlanır.

2.5. Kuantum Kriptografi

Bu bölümde kuantum kriptografi teorisi, uygulamaları, kuantum bilgisayarları ve bu bilgisayarların kriptografiye olan etkileri verilerek kuantum sonrası kriptografi ile ilgili güncel bilgiler sunulmaktadır.

2.5.1. Teorisi

Kuantum kriptografi ve kuantum hesaplama yeni bir araştırma alanı olup son zamanlarda çok yoğun bir şekilde çalışılmaktadır. Buradaki çalışmalar 1982 yılında ünlü fizikçi R. Feynman'ın kuantum mekaniği kavramlarının klasik bilgisayar ile simülasyonunun yapılamayacağının farkına varması ile başlamıştır. Feynman, kuantum bilgisayar ile ilgili bir örnek sunmamıştır fakat bundan sonra, bu konuda çalışmalar başlamış ve 1994 yılında P. Shor tarafından verilen kuantum polinom zamanlı bir çarpanlara ayırma algoritması bu alanda bir çığır açmıştır [8]. Kuantum bilgisayarlar, kuantum mekaniğindeki süperpozisyon ve dolanıklık gibi kavramları kulla-

nan bilgisayarlardır. Bu bilgisayarlar klasik bilgisayarlardan farklı olarak kuantum bitler üzerinde işlem yapmaktadır. Doğru ölçüm yapılması ile birlikte bu özellik klasik bilgisayar hesaplarının çok zor olduğu bazı problemleri kolay bir hale getirebilmektedir. Örneğin, büyük sayıların çarpanlara ayrılması klasik bilgisayarlarda alt üssel bir çalışma zamanda yapılabilmekteyken kuantum bilgisayarlarda Shor tarafından geliştirilen çarpanlara ayırma algoritması kullanarak polinom zamanda yapılabilmektedir. Bu özellik bilgisayar biliminde büyük bir gelişmedir ve bu alanda yeni bir dönem başlatmıştır.

İki boyutlu karmaşık sayılar üzerinde bir vektör uzayının dik baz elemanları $|0\rangle$ ve $|1\rangle$ olarak gösterilsin. Bu, uzayda birim vektöre bir kuantum bit veya kübit denir ve bunların doğrusal kombinasyonları diğer kübitleri oluşturur. Kübit bir birim vektör olduğu için a ve b karmaşık sayı olmak üzere

$$a|0\rangle + b|1\rangle, \quad |a|^2 + |b|^2 = 1$$

şeklinde gösterilir. Burada, ölçümler $|0\rangle$ veya $|1\rangle$ baz elemanına göre yapılmakta olup $|0\rangle$ kübitinin gözlenme olasılığı a^2 ve $|1\rangle$ kübitinin gözlenme olasılığı ise b^2'dir. Bu bir kübitin gösterimidir. Daha büyük boyutlarda gösterimler için örnek olarak üç kübitlik temel bir durum olan $|001\rangle$ kübitini düşünelim. Bunun üç parçacığı temsil ettiği düşünülebilir ve buradaki bitler parçacıkların yönünü temsil etmektedir. Dikkat edilirse burada toplam 8 farklı durum vardır ve 8 boyutlu uzayın elemanıdır. Kuantum bilgisayarlar, girdi olarak bu tip kübitlerin doğrusal kombinasyonlarını da alabilmektedir ve bu da sisteme aynı anda birçok hesabı yapabilme kabiliyeti vermektedir. Kuantum bilgisayarların klasik bilgisayarlara göre en önemli farkı bu özelliktir.

2.5.2. Uygulamalar

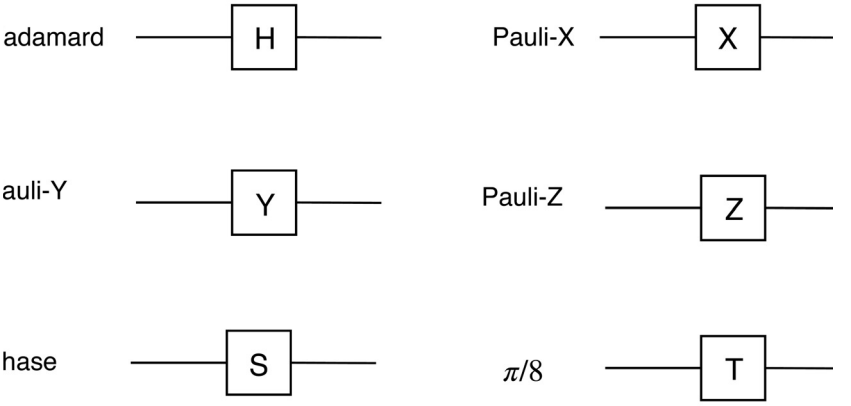
Kuantum mekaniğinin kriptografideki uygulamalarının başında kuantum anahtar değişimi gelir. Bir kuantum sisteminde haberleşmek isteyen tarafların ortak anahtar oluşturmak istediklerini varsayalım. Bunun için hem klasik bir kanal hem kuantum kanalı gerekmektedir. Kuantum kanalında çevresel etkileşimlerden etkilenmeden polarize olmuş fotonların değişimi yapılabilmektedir. Klasik kanalda ise sıradan mesajların iletimi yapılmaktadır. Sistem-

de B_1 ve B_2 olarak adlandırılan iki farklı baz vardır. *A* tarafı *B*'ye bir foton gönderir ve *B* bu fotonu rastgele seçtiği baz ile ölçer. Her bir foton için benzer bir ölçüm yapılır ve her bir ölçüm için seçilen baz kayıt edilir. Daha sonra seçilen bu bazların ne olduğu *A* tarafına iletilir. *A,* hangi bazların doğru olduğunu *B'ye* iletir ve her iki taraf daha sonra eşleşen bazlardaki ölçüm sonuçları üzerinde anlaşır ve bu bitler ortak anahtar olarak kullanılır. Bu sistemi kırmak isteyen ortadaki adamın fotonların kopyalanamaması ilkesinden dolayı iletilen fotonları gözlemleyebilmesi için ölçüm yapması gerekmektedir. Bu durumda kuantum mekaniği yasalarından dolayı, saldırgan iletilen fotonlarda hatalara sebep verir. *A* ve *B* tarafları bu durumu fark etmek için kontrol bitleri gönderir ve sistemin güvenliğinden emin olurlar. Günümüzde bu tekniğin uygulamasının deneyleri 100 km'lik fiber optik hat üzerinden yapılmaya başlanmıştır. Bu konudaki detaylar için [9] kitabı iyi bir kaynaktır.

2.5.3. Kuantum Bilgisayarlar

Günümüzde kuantum bilgisayarların geliştirilmesi üzerine Google, Intel ve IBM gibi özel kuruluşlar da dahil olmak üzere birçok şirket büyük bir çalışma yapmaktadır. Google, 72 kuantum bitlik kuantum işlemcilerin test edildiği bilgisini vermektedir. Bu konu ile ilgili tarihsel gelişmeler ve referanslar için [10]'a bakılabilir. Bu gelişmeler, yakın gelecekte büyük ölçekli kuantum bilgisayarların geliştirilmesinin mümkün olabileceği beklentisini yükseltmiştir. Örneğin, bu konuda önde gelen bilim insanı Michele Mosca, 2048 bitlik bir RSA algoritmasının 2027 yılına kadar kuantum bilgisayarı ile kırılma olasılığının 1/6 olduğunu 2017 yılında tahmin etmiştir [11].

Büyük ölçekli kuantum bilgisayarlar ile şu anda kullanılan açık anahtar kripto sistemler güvensiz hale gelecektir çünkü bu sistemlerin güvenliğinin dayandığı zor problemler büyük ölçekli kuantum bilgisayarlar ile kolaylıkla çözülmektedir. Simetrik sistemlerde ise, kuantum saldırılarına karşı aynı güvenlik seviyesini koruyabilmek için anahtar boyutlarını iki katına çıkarmaları yeterli olacaktır. Bundan dolayı klasik ve kuantum bilgisayarlar ile yapılan saldırılara dayanıklı yeni açık anahtarlı kripto sistemlerin tasarlanması üzerine çalışmalar başlamıştır. Yeni algoritmaların kuantum dayanıklılığını belirlemek için kuantum bilgisayarın ve kuantum algoritmların işleyişine ihtiyaç vardır.



Şekil 2.4. Temel kuantum kapıları

Kuantum bilgisayarlarının girdileri kübitlerdir ve karmaşık sayılar üzerindeki vektör uzayının elemanları olarak gösterilebildiği için sütun matris şeklinde gösterilebilirler. Kuantum bilgisayarlar bu girdileri alır, kuantum kapılarından oluşan kuantum devrelerinden geçirerek hesaplamaları yapar ve çıktı olarak kübit verir. Kuantum hesaplamalarda kullanılan başlıca kuantum kapılarının isimleri ve gösterimleri Şekil 2.4'te verilmiştir.

Bu kapıların tek kübitlik durum için matris gösterimleri ise şöyledir:

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, \quad \mathrm{X} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \quad \mathrm{Y} = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix},$$

$$\mathrm{Z} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \quad S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}, \quad T = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}.$$

Kübitler fonksiyonlarda hesaplanabilirler. Doğrusal kombinasyon gösterimi $\frac{1}{C}\sum_x |x>$ olan bir kübitin $f(x)$ fonksiyonda hesaplanması

$$\frac{1}{C}\sum_x |x, f(x)>$$

şeklinde gösterilir ve bu gösterim $f(x)$'in her x değerindeki hesaplanmasının karşılığını içerir. Bir ölçme yapıldığında rastgele bir x_0 değeri için $|x_0, f(x_0)>$ elde edilir. Tüm diğer durumlar ise ortadan kaybolur. Bu da kuantum bilgisayarları ile hesap yaparken doğru ölçmenin önemini göstermektedir.

Kuantum bilgisayarlar ile çarpanlara ayırma probleminin polinom zamanda çözülebileceğini gösteren Shor, kuantum Fourier

dönüşümünü kullanmıştır. Burada kullanılan kuantum Fourier dönüşümü aşağıdaki gibi tanımlanır.

$$QFT(|x>) = \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m} e^{\frac{2\pi i c x}{2^m}} |c> .$$

Bu dönüşüm dizilerin frakanslarını ölçer ve böylece dizinin periyodunun bulunmasına katkıda bulunur. Burada ölçüm yapılırken sistemin hepsinde ölçüm yapılması yerine ikinci yarısındaki değerler üzerinde ölçüm yapılır. Sonuç olarak, çarpanlara ayırma probleminde bu dönüşüm, *n* sayısı çarpanlarını bulmaya çalıştığımız sayı olmak üzere *n*'den küçük *a* ve *r* sayılarını $a^r \equiv 1 \, mod \, n$ şartını sağlayacak şekilde bulunmasını sağlar. Daha sonra üst çarpanlara ayırma metodu ile *n*'nin çarpanları sürekli kesirler tekniği ile birlikte kullanılarak bulunur.

2.5.4. Kriptografiye Etkisi ve Kuantum Sonrası Kriptografi

Kuantum bilgisayarlar, çarpanlara ayırma ve ayrık logaritma problemi gibi günümüzde kullanılan açık anahtarlı kriptografik sistemlerin güvenliklerinin dayandığı zor problemleri kolayca çözer. Bundan dolayı pratikte kullanılan anahtar boylarını kırabilecek büyük ölçekli kuantum bilgisayarlar inşa edilmeden önce bu sistemler kuantum saldırılarına dayanıklı sistemler ile değiştirilmelidir. Hem klasik hem kuantum bilgisayarları ile yapılan saldırılara dayanıklı kriptografiye kuantum sonrası kriptografi denmektedir. Kuantum sonrası açık anahtarlı kriptografi için genellikle beş ayrı metot kullanılmaktadır. Bunlar:

- latis tabanlı,
- kod tabanlı,
- özetleme fonksiyonu tabanlı ve
- süper tekil izojen tabanlı,
- çok değişkenli ikinci derece polinom tabanlı

kriptosistemlerdir. Bu alanlarda birçok yeni algoritma önerisi olmasına rağmen bu algoritmalar göreceli olarak daha yeni oldukları için güvenlik analizlerinin yapılması halen devam etmektedir. Güvenlikleri yeterince çalışılmış ve günlük hayatta kullanılabilen yeni nesil açık anahtarlı kriptografik algoritma belirlemek amacıyla Amerika Birleşik Devletleri'nin Ulusal Standart Teknolojisi Enstitüsü (NIST) kurumu yeni bir standartlaşma süreci [4] başlatmıştır.

Bir kaç yıl sürecek olan bu süreç sonunda yeni açık anahtarlı kriptografik sistemlerin kullanılabilir olması beklenmektedir. Bu süreç için başvurular Kasım 2017'de bitmiştir ve 82 başvurunun 69 tanesi uygun olarak görülmüştür. Daha sonra 5 başvuru geri çekilmiş ve toplam 64 algoritma ilk aşamada değerlendirilmiştir. Bu başvuruların alanlara göre dağılımı Tablo 2.1'de verilmiştir.

Tablo 2.1. NIST kuantum sonrası kriptografi 1. tur başvuruları

Yaklaşım	Şifreleme	İmzalama	Toplam
Latis tabanlı	21	5	26
Kodlama tabanlı	17	2	19
Çok değişkenli	2	7	9
Özetleme tabanlı		3	3
Diğer	5	2	7
Toplam	45	19	64

NIST 1. tur başvuru aşamasını tamamladıktan sonra 30 Ocak 2019 tarihine kadar değerlendirme süreci yapmıştır. Bu süreçte algoritmalar başlıca üç kritere göre değerlendirilmiştir. Bunlar güvenlik, maliyet ve performans ve algoritma karakteristiği olarak belirtilmiştir. Ocak 2019 tarihinde 2. tura 24 başvurunun kaldığı açıklanmıştır [12]. Bunlar ve hangi tip yaklaşım oldukları Tablo 2.2'de verilmiştir.

Tablo 2.2. NIST kuantum sonrası kriptografi 2. tur algoritmaları

Yaklaşım	Şifreleme	İmzalama
Latis tabanlı	CRYSTAL-KYBER, FrodoKEM, LAC, New Hope, NTRU, NTRU Prime, Round 5, SABER, Three Bears	CRYSTALS-DILITHIUM, FALCON, q-TESLA
Kodlama tabanlı	Classic McEllice, NTS-KEM, BIKE, HQC, LEDAcrypy, Rollo, RQC	
Çok değişkenli		GEMSS, LUOV, MQDSS, Rainbow
Özetleme tabanlı		Picnic, SPHINCS+
İzojen tabanlı	SIKE	

Birinci turda başvuru yapan bazı benzer algoritmalar NIST'ın teşvikleri ile başvuru yapan takımlar tarafından birleştirilmiştir. Örneğin, NTRUEncrypt ve NTRU-HRSS-KEM birleştirilmiş ve NTRU ismini almıştır. Benzer şekilde HILA5 ve Round2 başvuruları birleştirilerek Round 5 adını almıştır. LEDACrypt algoritması, LEDAkem ve LEDApkc'nin ve Rollo algoritması ise LAKE, LOCKER ve Ouroboros-R'un birleşmesidir.

2.6. Değerlendirmeler

Bu bölümde kriptografinin siber güvenlikteki önemi ve saldırılara karşı önlem alırken nasıl kullanıldığının üzerinde durulmuş ve internet güvenliği, kablosuz ağ güvenliği, bulut güvenliği, nesnelerin interneti güvenliği ve parola güvenliği gibi seçilmiş bazı konular ile ilgili bilgiler verilmiştir. Ayrıca yakın gelecekte kullanılmaya başlanması beklenen büyük ölçekli kuantum bilgisayarların bilgi ve iletişim güvenliğine olan etkileri ve buna karşı yapılan çalışmalar ve kuantum sonrası kriptografi hakkında bilgiler verilmiştir. Anlatılan uygulamaların dışında da kriptografinin güvenlikte birçok uygulaması vardır. Örnek olarak, elektronik veya internet seçim, çok katılımlı güvenli hesaplamalar, bit anlaşmaları, mobil haberleşme güvenliği ve akıllı kart güvenliği gibi uygulamalar verilebilir.

Görüldüğü gibi kriptografi bilgi ve iletişim güvenliğinde karşı önlem almak için kullanılan önemli bir teknik araçtır. Fakat bilinmesi gereken en önemli noktalardan bir tanesi kriptografinin her derde bir çare olmadığıdır. En güvenli kriptografik algoritmalar ile şifrelemelerin kullanıldığı bir sistem kötücül bir yazılıma karşı veya sosyal mühendislik kullanılarak yapılan saldırılara karşı sistemleri koruyamaz. Sonuç olarak siber güvenlik çok yönlü bir konu olup kriptografi, teknik olarak karşı önlem sağlayan en önemli araçlardan bir tanesidir.

Kaynaklar

[1] Lars R. Knudsen, and Matthew Robshaw. The block cipher companion. Springer Science & Business Media, 2011.

[2] Klein, Andreas. Stream ciphers. London: Springer, 2013.

[3] Steven D. Galbraith. Mathematics of public key cryptography. Cambridge University Press, 2012.

[4] Post-Quantum Cryptography, https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions adresinden Ocak 2019 tarihinde alınmış.

[5] Bart Preneel. Analysis and design of cryptographic hash functions. Diss. Katholieke Universiteit te Leuven, 1993.

[6] Xun Yi, Russell Paulet, and Elisa Bertino. Homomorphic encryption and applications. Vol. 3. Heidelberg: Springer, 2014.

[7] Lightweight Cryptography, https://csrc.nist.gov/projects/lightweight-cryptography adresinden Ocak 2019 tarihinde alınmış.

[8] Peter W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring." Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. IEEE, 1994.

[9] Michael A. Nielsen; Isaac L. Chuang (9 December 2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press. ISBN 978-1-139-49548-6.

[10] Timeline of quantum computing, InWikipedia, https://en.wikipedia.org/wiki/Timeline_of_quantum_computing adresinden Ocak 2019 tarihinde alınmış.

[11] Michele Mosca, Cybersecurity in an Era with Quantum Computers: Will We Be Ready?, IEEE Security & Privacy, 16(5): 38-41, 2018.

[12] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Yi-Kai Liu, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8240, 2019.

Kriptografik Test Yöntemleri ve Kriptoanaliz

BÖLÜM 3

Muharrem Tolga SAKALLI

KRİPTOGRAFİK TEST YÖNTEMLERİ VE KRİPTOANALİZ

Bu bölümde kriptografik bileşenlerin/algoritmaların güvenlik seviyelerinin değerlendirilmesinde kullanılan doğrusal olmama (non-linearity), cebirsel derece (algebraic degree), cebirsel dayanıklılık (algebraic immunity), korelasyon dayanıklılık ve esneklik (correlation immunity and resiliency), çığ (avalanche), katı çığ (strict avalanche), doğrusal yaklaşım tablosu (linear approximation table), fark dağılım tablosu (difference distribution table) ve dal sayısı (branch number) gibi kriptografik test yöntemlerinin bir incelemesine yer verilmektedir. Buna ek olarak kriptografik algoritmaların dayanıklılığının incelenmesinde kullanılan ve kriptografik algoritmalara karşı saldırı bilimi olarak ta bilinen kriptoanaliz hakkında temel bir alt yapı sunulmaktadır. Bu konu ile ilgili olarak AES (Advanced Encryption Standard) blok şifresinin tasarımında göz önüne alınan iki önemli saldırı tekniği doğrusal ve diferansiyel kriptoanaliz detaylandırılmaktadır.

3.1. Giriş

Kriptografi, verinin güvenli ve genellikle gizli bir formda depolanmasını ve iletilmesini sağlayan yöntemler bütünüdür, böylece veri istenen kişiler tarafından okunabilir veya işlenebilir. Kriptoanaliz ise kriptografik yapıların kırılmasında kullanılan tekniklerin çalışılması anlamına gelmektedir. Bilgi güvenliğinin üç temel hedefi sırasıyla gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirliktir (availability). Gizlilik bilginin iletimi sırasındaki gizliliğini, bütünlük bilginin yetkili kişiler tarafından değiştirilmesi gereklili-

ğini ve kullanılabilirlik ise oluşturulan veya depolanan bilginin yetkili birimler tarafından kullanılabilir olmasını ifade eder. Bu güvenlik hedeflerinin sağlanabilmesi için (diğer bir deyişle güvenlik hedeflerini tehdit eden saldırıların engellenebilmesi için) ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) tarafından çeşitli güvenlik servisleri ve bu servislerde kullanılan çeşitli mekanizmalar öne sürülmüştür. Bu mekanizmalardan biri olan şifreleme ile veri gizliliği, veri bütünlüğü ve kimlik denetimi güvenlik servislerinin yerine getirilmesi sağlanmaktadır. Kriptografik özet (hash) fonksiyonları veri bütünlüğü, kimlik denetimi servislerinde ve sayısal imza mekanizmasında önemli bir rol üstlenirler. Bu nedenle kriptografi ve kriptoanalizi kapsayan kriptoloji bilimi verinin korunması veya güvenli bir şekilde iletilmesinde kullanılan kriptografik algoritmaların/yapıların tasarımı veya güvenlikleri ile ilişkilidir. Güvenliği tehdit eden saldırılar, güvenlik servisleri ve güvenlik servislerinde kullanılan mekanizmalar hakkında daha detaylı bilgi [1]'den elde edilebilir.

Şifreleme algoritmaları, simetrik ve asimetrik algoritmalar olmak üzere 2 ana gruba ayrılır. Simetrik şifreleme algoritmaları, aynı gizli anahtarın şifreleme ve şifre çözme işlemlerinde kullanıldığı algoritmalardır ve asimetrik şifreleme algoritmalarına göre daha hızlı olan algoritmalardır. Simetrik şifreleme algoritmaları blok şifreler ve akış şifreler olmak üzere 2 alt guruba ayrılır. Blok şifreler açık metin karakterlerini bloklar şeklinde şifrelerken, akış şifreler açık metin karakterlerini (bit veya byte karakter) ayrı ayrı şifreler. Blok şifreler için önemli örnekler olarak DES (Data Encryption Standard) [2] ve AES (Advanced Encryption Standard) [3] blok şifreleme algoritmaları verilebilir. Akış şifreleme algoritmalarına önemli örnekler ise A5/1 [4], RC4 [5] ve son zamanlarda geliştirilen Trivium [6] ve HC-256 [7] şifreleri şeklindedir. Asimetrik şifreleme algoritmaları açık metnin şifrelenmesinde açık bir anahtar, şifre çözme işleminde gizli (özel) bir anahtar kullanır ve bu şifreleme grubuna giren önemli bir örnek RSA (Rivest-Shamir-Adleman) [1] şifreleme algoritmasıdır. Simetrik şifreleme algoritmalarının (örneğin blok şifreler) harddisk verisi gibi büyük verilerin şifrelenmesinde kullanılmaları daha uygundur. Diğer yandan asimetrik algoritmaların en önemli özelliği

simetrik algoritmaların en büyük problemi olan anahtar dağıtımında rol üstlenmeleri ve çözüm getirmeleridir. Asimetrik algoritmaların simetrik şifreleme yöntemlerine göre daha yavaş olması, şifreleme ve şifre çözme işlemlerinde sırasıyla açık bir anahtar ve gizli (özel) bir anahtar kullanması nedenleriyle daha küçük verilerin (örneğin gizli anahtarın) şifrelenmesinde kullanılmaları daha uygundur. Kriptografik özet fonsiyonları ise giriş verisinden bağımsız olarak sabit uzunlukta bir özet elde edilmesini sağlayan fonksiyonlardır. Bu fonksiyonların web uygulamalarında kullanıcı şifrelerinin veritabanında özetlerinin tutulması, verinin bütünlüğünün korunması, sayısal imza ve Bitcoin uygulamaları gibi önemli uygulama alanları bulunmaktadır. Kriptografik özet fonksiyonlarının önemli özellikleri tek yönlü fonksiyon olmaları ve giriş verisinden bağımsız sabit uzunlukta özet elde edilmesinde kullanılmalarıdır. Dolayısıyla kriptografik özet fonksiyonları ile üretilen özetlerde aynı özete sahip metinler bulunabileceğinden bu fonksiyonların çakışma saldırılarına (collision attack) [8] karşı dayanıklı olmaları gereklidir. Kriptografik algoritmalarda/yapılarda kullanılan bileşenlerin dayanıklılığının belirlenmesinde kullanılan ölçütler, kriptografik algoritmaya/yapıya olan kriptoanaliz saldırıları ile yakından ilişkilidir. Örneğin doğrusal olmama ölçütü, doğrusal olmayan bir kriptografik bileşenin doğrusal saldırılara karşı dayanıklılığının bir ölçümünü yapmayı hedefler.

Bu bölümde akış şifrelerde ve blok şifrelerde kullanılan kriptografik bileşenlerin doyurması gereken kriptografik özelliklere yönelik test yöntemleri incelenmektedir. Akış şifrelerin tasarımında kullanılan boole fonksiyonları, blok şifrelerde kullanılan yerdeğiştirme kutuları ya da vektörel boole fonksiyonları, çoğu blok şifrede doğrusal dönüşüm (veya bir bileşeni) olarak kullanılan maksimum uzaklıkta ikili (maximum distance binary) matrisler ve maksimum uzaklıkta ayrılabilen (maximum distance separable) matrisler merkezinde kriptografik ölçütlerin testlerine yönelik bir altyapı sunulmaktadır. Bahsedilen kriptografik bileşenler özet fonksiyonlarında da kullanılabileceğinden bu bölümde sunulan kriptografik ölçütlerin test yöntemleri, özet fonksiyonlarını da yakından ilgilendirmektedir. Diğer yandan tasarlanan kriptografik bir algoritmada/yapıda (örneğin

blok şifre) kullanılan kriptografik bileşenlerin kriptografik testlerden iyi sonuçlar vermesi kriptografik algoritmanın/yapının sağlamlığının değerlendirilmesinde yeterli olmayabilir. Tasarlanan toplamdaki yapının (örneğin blok şifrenin) çeşitli kriptanalitik saldırılara (en azından doğrusal [9] ve diferansiyel kriptoanaliz [10] saldırılarına) karşı dayanıklı olması gerekir. Buna ek olarak açık metinlerden elde edilecek şifreli metinlerin iyi rassal özellikler gösterdiği frekans testi, blok testi, blok frekans testi, bloktaki en uzun birler testi, matris rank testi gibi istatistiksel testler [11] ile doğrulanmalıdır.

3.2. Boole Fonksiyonları için Kriptografik Test Yöntemleri

Kriptografide boole fonksiyonları birçok simetrik şifreleme algoritmasının tasarımında önemli rol oynamaktadır. Akış şifrelerin tasarımında doğrusal olmayan bileşim üreteçleri (non-linear combination generators) [12] ve doğrusal olmayan filtre üreteçleri (non-linear filter generators) [12] doğrusal geri beslemeli saklayıcı/saklayıcılar (Linear Feedback Shift Register-LFSR) ile doğrusal olmama özelliği yüksek boole fonksiyonlarını kullanırlar. Blok şifrelerde kullanılan yerdeğiştirme kutuları ya da S-kutuları (Substitution boxes) doğrusal olmayan boole fonksiyonlarının birleşiminden oluşmaktadır. Özellikle akış şifre uygulamalarında kendine yer bulan boole fonksiyonları için önemli kriptografik ölçütler aşağıdaki gibi verilebilir:

- Dengeli Olma (Balanced),
- Doğrusal Olmama (Non-linearity),
- Cebirsel Derece (Algebraic Degree),
- Cebirsel Dayanıklılık (Algebraic Immunity),
- Korelasyon Dayanıklılık ve Esneklik (Correlation Immunity and Resiliency).

Yukarıda verilen ölçütlerden doğrusal olmama ölçütü, doğrusal yapıların (doğrusal kriptoanaliz ile) kolaylıkla kırılabilmesinden ötürü test edilmesi gereken belki de en önemli ölçüttür. Cebirsel de-

rece ölçütü Berlekamp-Massey saldırısına [13], korelasyon dayanıklılık ve esneklik ölçütü korelasyon saldırılarına [14], cebirsel dayanıklılık ölçütü ise cebirsel ve hızlı cebirsel saldırılarına [15] karşı bir boole fonksiyonunun kullanımında test edilmesi gereken diğer önemli ölçütlerdir.

Bir boole fonksiyonu f, [1] F_2^m'den elemanları 0 ve 1 olan sonlu cisim F_2'ye bir haritalama olarak tanımlanır [13][16] ve bir doğruluk tablosu (truth table) ile gösterilebilir.

Doğruluk tablosu, $f(x) = (f(00..00), f(00..01)....., f(11..11))$ şeklinde sıralanan f'nin fonksiyon değerlerini gösteren bir vektördür. Bir $f(x)$ boole fonksiyonunu temsil etmenin diğer bir yolu ise polinomsal bir gösterim biçimi (AND ve XOR işlemleri ile gösterim) olan cebirsel gösterim biçimi ANF (Algebraic Normal Form)'dir ve aşağıdaki gibi ifade edilebilir [17]:

$$f(x)= f(x_1,x_2,..,x_m) = a_0 \oplus \sum_{1\le i\le m} a_i x_i \oplus \sum_{1\le i<j\le m} a_{i,j} x_i x_j \oplus \cdots \oplus a_{1,2,\ldots,m} x_1 x_2 \cdots x_m$$

Yukarıda verilen bir $f(x)$ boole fonksiyonu için ANF formunda $a_0, a_1, \ldots, a_{1,2,\ldots,m} \in F_2$ olmak üzere ifadedeki çarpımlar AND işlemini temsil etmektedir. Algoritma 3.1'de doğruluk tablosu verilen bir f boole fonksiyonu için ANF gösteriminin elde edilmesine yönelik ANF algoritması verilmiştir.

Algoritma 3.1: ANF Algoritması

1. $g(x_1,....., x_m) = f(0,0,..,0)$ değerini ata.
2. $k = 1$'den $2^m - 1$ değerine kadar yap.
   a- Tamsayı k'nın ikili temsilini kullan
   $(k = b_1 + b_2 2 + b_3 2^2 + ... + b_m 2^{m-1})$

[1] F_2^m: F_2 üzerine m boyutlu vektör uzayı

b- Eğer $g(b_1, b_2, ..., b_m) \neq f(b_1, b_2, ..., b_m)$ ise
$g(x_1, ..., x_m) = g(x_1, ..., x_m) \oplus \prod_{i=1}^{m} (x_i)^{b_i}$ değerini ata.

3. $ANF(f) = g(x_1, ..., x_m)$

Örnek 3.1: $F_2^3 \rightarrow F_2$'ye $f_1(x_1, x_2, x_3) = \{0,1,1,1,1,0,0,0\}$ boole fonksiyonu için Algoritma 3.1 kullanılarak ANF gösteriminin elde edilmesi adım adım aşağıdaki gibi verilebilir.

k	b_1	b_2	b_3	$f(b_1, b_2, b_3)$	$g(b_1, b_2, b_3)$
	0	0	0	0	0
1	0	0	1	1	x_3
2	0	1	0	1	$x_3 \oplus x_2$
3	0	1	1	1	$x_3 \oplus x_2 \oplus x_2x_3$
4	1	0	0	1	$x_2 \oplus x_3 \oplus x_2x_3 \oplus x_1$
5	1	0	1	0	$x_2 \oplus x_3 \oplus x_2x_3 \oplus x_1$
6	1	1	0	0	$x_2 \oplus x_3 \oplus x_2x_3 \oplus x_1$
7	1	1	1	0	$x_2 \oplus x_3 \oplus x_2x_3 \oplus x_1$

Bir $f(x)$ boole fonksiyonunun Hamming ağırlığı $wt(f(x))$ doğruluk tablosundaki 1'lerin sayısı olarak tanımlanır. Örnek 3.1'de verilen $f(x)$ boole fonksiyonunun Hamming ağırlığı 4'tür.

Bir boole fonsiyonu $f(x): F_2^m \rightarrow F_2$ için doğruluk tablosundaki 0'ların sayısı 1'lerin sayısına eşitse boole fonksiyonu için dengeli denir. Dengeli bir boole fonsiyonu için Hamming ağırlığı 2^{m-1}'dir. Örnek 3.1 de verilen $f_1(x)$ boole fonksiyonu dengelidir çünkü $f_1(x)$ boole fonksiyonunun Hamming ağırlığı ($m = 3$ olduğundan) $2^{m-1} = 2^{3-1} = 4$'tür.

$f(x), g(x): F_2^m \rightarrow F_2$ iki boole fonksiyon olmak üzere bu fonsiyonların arasındaki Hamming uzaklığı $d_H(f, g)$ doğruluk tablolarında farklılaştıkları pozisyonların sayısı olarak tanımlanır ve $(f(x) \oplus g(x))$'in doğruluk tablosunun (iki boole fonksiyonunun

XOR toplamının) Hamming ağırlığı olarak $d_H(f,g) = wt(f(x) \oplus g(x))$ şeklinde ifade edilir.

Örnek 3.2: İki boole fonksiyonu $f_2(x_1,x_2,x_3) = \{0,0,1,1,1,0,1,0\}$ ve $g_1(x_1,x_2,x_3) = \{1,1,1,0,0,0,0,1\}$ için Hamming uzaklığı $d_H(f_2,g_1)$, $wt(f_2(x) \oplus g_1(x)) = 6$ olarak aşağıda gösterildiği gibi elde edilebilir.

x_1	x_2	x_3	$f_2(x)$	$g_1(x)$	$f_2(x) \oplus g_1(x)$
0	0	0	0	1	1
0	0	1	0	1	1
0	1	0	1	1	0
0	1	1	1	0	1
1	0	0	1	0	1
1	0	1	0	0	0
1	1	0	1	0	1
1	1	1	0	1	1

Bir $f(x)$ boole fonksiyonu eğer $f(x) = x \bullet w \oplus c$ formunda temsil ediliyorsa bu fonksiyona doğrusal (affine) fonksiyon denir. Boole fonksiyonu ifadesinde

$x \bullet w = \bigoplus_{i=1}^{m} x_i.w_i = x_1.w_1 \oplus x_2.w_2 \oplus \ldots\ldots \oplus x_m.w_m$ ikili değere sahip vektörlerin ($x, w \in F_2^m$) nokta ürününü ve c ikili sabiti temsil eder ($c \in F_2$). Doğrusal fonksiyonlara 1. Dereceden fonksiyon da denir. Örneğin $f_3(x) = f_1(x_1,x_2,x_3) = x_1 \oplus x_2$ boole fonksiyonu doğrusal (1. Dereceden) bir fonsiyon iken $f_4(x) = f_2(x_1,x_2,x_3) = x_1 \oplus x_2 \oplus x_1x_2$ boole fonksiyonu ikinci dereceden bir fonksiyondur ve doğrusal değildir.

Bir $f(x)$ boole fonksiyonunun doğrusal olmama değeri, bu boole fonksiyonunun tüm doğrusal fonksiyonlar kümesine olan minimum Hamming uzaklığı olarak tanımlanır. Bir $f(x)$ boole fonksiyonunun doğrusal olmama değeri N_f aşağıdaki gibi gösterilebilir:

$$N_f = \min_{a \in A_m} d_H(f,a) = \min_{a_1,\ldots,a_m,c \in \{0,1\}} \#\left\{ x \mid f(x) \neq \bigoplus_{i=1}^{m} a_i x_i \oplus c \right\}.$$

N_f doğrusal olmama değerinin gösteriminde kullanılan $A_m = \{ a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_m x_m ; a_i \in F_2,\ 0 \le i \le m \}$ tüm doğrusal fonksiyonlar kümesini ve $\#\{K\}$ ifadesi K bir küme olmak üzere K kümesinin eleman sayısını ifade etmektedir.

Örnek 3.3: Örnek 3.1'de verilen boole fonksiyonu $f_1(x_1, x_2, x_3) = \{0,1,1,1,1,0,0,0\}$ için doğrusal olmama değeri aşağıdaki gibi elde edilebilir.

$F_2^3 \to F_2$'ye tanımlı boole fonksiyonu $f_1(x)$'in doğrusal olmama değerinin elde edilebilmesi için $f_1(x)$ boole fonksiyonunun $F_2^3 \to F_2$'ye tüm doğrusal fonksiyonlara olan Hamming uzaklığının minimum değerinin bulunması gerekmektedir. $F_2^3 \to F_2$'ye tanımlı tüm olası doğrusal fonksiyonlar ($\bar{0} = (0,0,\ldots 0)$ ve $\bar{1} = (1,1,\ldots 1)$ olmak üzere) Tablo 3.1'de verilmektedir.

Tablo 3.1. $F_2^3 \to F_2$'ye Tüm Doğrusal Fonksiyonlar Kümesi

$a_1(x) = \bar{0}$	$a_9(x) = \bar{1}$
$a_2(x) = x_1$	$a_{10}(x) = 1 \oplus x_1$
$a_3(x) = x_2$	$a_{11}(x) = 1 \oplus x_2$
$a_4(x) = x_3$	$a_{12}(x) = 1 \oplus x_3$
$a_5(x) = x_1 \oplus x_2$	$a_{13}(x) = 1 \oplus x_1 \oplus x_2$
$a_6(x) = x_1 \oplus x_3$	$a_{14}(x) = 1 \oplus x_1 \oplus x_3$
$a_7(x) = x_2 \oplus x_3$	$a_{15}(x) = 1 \oplus x_2 \oplus x_3$
$a_8(x) = x_1 \oplus x_2 \oplus x_3$	$a_{16}(x) = 1 \oplus x_1 \oplus x_2 \oplus x_3$

Örnek olarak $f_1(x)$ boole fonksiyonun $a_6(x) = x_1 \oplus x_3$ doğrusal fonksiyonuna olan Hamming uzaklığı $d_H(f_1, a_6) = wt(f_1(x) \oplus a_6(x)) = 2$ olarak Tablo 3.2'de gösterildiği gibi elde edilebilir.

Tablo 3.2. Hamming Uzaklığı Sonuçları

x_1	x_2	x_3	$f_1(x)$	$a_6(x)=x_1\oplus x_3$	$f_1(x)\oplus a_6(x)$
0	0	0	0	0	0
0	0	1	1	1	0
0	1	0	1	0	1
0	1	1	1	1	0
1	0	0	1	1	0
1	0	1	0	0	0
1	1	0	0	1	1
1	1	1	0	0	0

Tablo 3.3'de $f_1(x)$ boole fonksiyonunun tüm olası doğrusal fonksiyonlara uzaklıkları listelenmektedir.

Tablo 3.3. Boole fonksiyonu $f_1(x)$'in $F_2^3 \to F_2$'ye Tüm Doğrusal Fonksiyonlar Kümesine Olan Hamming Uzaklıklarının Listesi

$d_H(f_1,a_1)=4$	$d_H(f_1,a_9)=4$
$d_H(f_1,a_2)=6$	$d_H(f_1,a_{10})=2$
$d_H(f_1,a_3)=4$	$d_H(f_1,a_{11})=4$
$d_H(f_1,a_4)=4$	$d_H(f_1,a_{12})=4$
$d_H(f_1,a_5)=2$	$d_H(f_1,a_{13})=6$
$d_H(f_1,a_6)=2$	$d_H(f_1,a_{14})=6$
$d_H(f_1,a_7)=4$	$d_H(f_1,a_{15})=4$
$d_H(f_1,a_8)=2$	$d_H(f_1,a_{16})=6$

Sonuç olarak boole fonksiyonu $f_1(x)$'in doğrusal olmama değeri $N_{f_1}=2$ olarak elde edilir (Tablo 3.3'de verilen tüm doğrusal fonksiyonlar kümesine Hamming uzaklık değerlerinden en küçük olan değerdir).

Not 3.1. Bir boole fonksiyonunun doğrusal olmama özelliğinin testinde $A_m=\{\, a_0\oplus a_1x_1\oplus a_2x_2\oplus\ldots\oplus a_mx_m;\, a_i\in F_2,\ 0\le i\le m\,\}$ tüm doğrusal fonksiyonlar kümesinden $a_0=1$ içeren doğrusal fonksiyonlara olan Hamming uzaklıklarının elde edilmesine gerek yoktur. Örneğin Örnek 3.3'te verilen boole fonksiyonunun doğrusal olmama değerinin hesaplanması sırasında kullanılan Tablo 3.2'nin sol

tarafında bulunan Hamming uzaklıklarının hesaplanması yeterlidir.

Not 3.2. $F_2^m \to F_2$'ye tanımlı Bent fonksiyonları [13][18] m çift bir değer olmak üzere maksimum doğrusal olmama değeri $2^{m-1} - 2^{\frac{m}{2}-1}$'e sahiptir.

Bir $f(x)$ boole fonksiyonunun cebirsel derecesi $\deg(f)$, $f(x_1, x_2, ..., x_m)$ boole fonksiyonunun ANF formundaki terimlerinde, çarpım durumunda bulunan ve birbirinden farklı giriş değişkenlerinin maksimum sayısı olarak ifade edilir.

Örnek 3.4. Örnek 3.1'de verilen boole fonksiyonunun ANF formundaki ifadesi $f_1(x) = x_1 \oplus x_2 \oplus x_3 \oplus x_2 x_3$ şeklinde elde edilmişti. Bu boole fonksiyonunun cebirsel derecesi, çarpım durumunda 2 değişken olduğu için ($x_2 x_3$) 2'dir.

$F_2^m \to F_2$'ye bir $f(x)$ boole fonksiyonunun cebirsel dayanıklılığı $f(x) \bullet g(x) = \overline{0}$ ya da $(f(x) \oplus \overline{1}) \bullet g(x) = \overline{0}$ yapan $F_2^m \to F_2$'ye tanımlı $g(x)$ fonksiyonunun ($g \neq \overline{0}$) en düşük derecesidir. $f \bullet g = \overline{0}$ olacak şekilde ifadeyi sağlayan $g(x)$ fonksiyonuna $f(x)$'in bir bozucusu (annihilator) adı verilir. An(*f*), $f(x)$'in tüm bozucularının kümesini tanımlar [13] [19].

Örnek 3.5. Örnek 3.1'de verilen boole fonksiyon $f_1(x) = \{0,1,1,1,1,0,0,0\}$ için An(f_1) fonksiyonu aşağıdaki gibi gösterilebilir ("*" yerine 0 ya da 1 değeri konabilir).

x_1	x_2	x_3	$f_1(x)$	$An(f_1)$
0	0	0	0	*
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	*
1	1	0	0	*
1	1	1	0	*

Eğer bir $f(x)$ boole fonksiyonunun *t* giriş bitinin kombinasyonu istatistiksel olarak bağımsız ise $f(x)$ boole fonksiyonuna *t*. dereceden korelasyon dayanıklı denir ve bu özellik CI (*t*) olarak ifade edilir [20]. Diğer bir deyişle $f(x)$ boole fonksiyonunun $x_{i_1},.....,x_{i_r}$, $i \le r \le t$ giriş bitlerinin herhangi bir kombinasyonu (0 veya 1 değerine) sabitlenirse elde edilecek yeni boole fonksiyonlarında 0 ve 1'lerin sayılarının eşit olması gerekir: Dengeli ve *t*. dereceden korelasyon dayanıklılığına sahip bir $f(x)$ boole fonksiyonu, *t*. dereceden esnek (resilient) olarak isimlendirilir.

Örnek 3.6. Örnek 3.1'de verilen dengeli $f_1(x) = \{0,1,1,1,1,0,0,0\}$ boole fonksiyonunun 1. dereceden korelasyon dayanıklılığının testi aşağıdaki gibi verilebilir.

Boole fonksiyon $f_1(x)$'in ANF formundaki ifadesi $f_1(x) = x_1 \oplus x_2 \oplus x_3 \oplus x_2x_3$ olarak Örnek 3.1'de elde edilmişti. Bu boole fonksiyonunun 1. Dereceden korelasyon dayanıklı olabilmesi için tanım gereği aşağıda verilen eşitliklerin sağlanması gerekir:

$$\#\left\{x \in F_2^m \mid f_1(0,x_2,x_3) = 0\right\} = \#\left\{x \in F_2^m \mid f_1(0,x_2,x_3) = 1\right\},$$
$$\#\left\{x \in F_2^m \mid f_1(1,x_2,x_3) = 0\right\} = \#\left\{x \in F_2^m \mid f_1(1,x_2,x_3) = 1\right\},$$
$$\#\left\{x \in F_2^m \mid f_1(x_1,0,x_3) = 0\right\} = \#\left\{x \in F_2^m \mid f_1(x_1,0,x_3) = 1\right\},$$
$$\#\left\{x \in F_2^m \mid f_1(x_1,1,x_3) = 0\right\} = \#\left\{x \in F_2^m \mid f_1(x_1,1,x_3) = 1\right\},$$
$$\#\left\{x \in F_2^m \mid f_1(x_1,x_2,0) = 0\right\} = \#\left\{x \in F_2^m \mid f_1(x_1,x_2,0) = 1\right\},$$
$$\#\left\{x \in F_2^m \mid f_1(x_1,x_2,1) = 0\right\} = \#\left\{x \in F_2^m \mid f_1(x_1,x_2,1) = 1\right\}.$$

Eşitlikler sonucu elde edilecek yeni boole fonksiyonlar aşağıdaki gibi ifade edilebilir:

$f_1(0,x_2,x_3) = x_2 \oplus x_3 \oplus x_2x_3$	$f_1(x_1,1,x_3) = 1 \oplus x_1$
$f_1(1,x_2,x_3) = 1 \oplus x_2 \oplus x_3 + x_2x_3$	$f_1(x_1,x_2,0) = x_1 \oplus x_2$
$f_1(x_1,0,x_3) = x_1 \oplus x_3$	$f_1(x_1,x_2,1) = 1 \oplus x_1$

Elde edilen yeni boole fonksiyonlarından $f_1(0,x_2,x_3) = x_2 \oplus x_3 \oplus x_2x_3$ ve $f_1(1,x_2,x_3) = 1 \oplus x_2 \oplus x_3 \oplus x_2x_3$

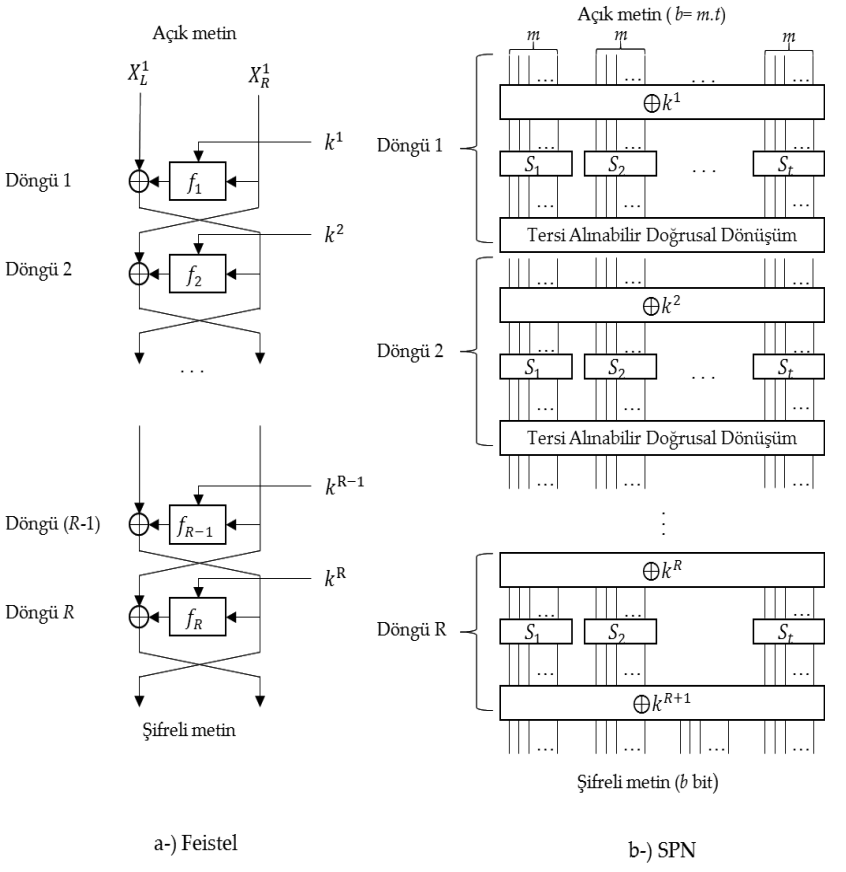
dengeli boole fonksiyonları değildir. Diğer bir deyişle boole fonksiyonlarındaki 0'ların ve 1'lerin sayısı birbirine eşit değildir. Bu nedenle verilen $f_1(x)$ boole fonksiyonu korelasyon dayanıklı değildir.

3.3. Blok Şifrelerde Kullanılan Kriptografik Bileşenler

Blok şifreler, gizli bir anahtar yardımıyla sabit uzunlukta açık metin blokları (açık metin sabit uzunlukta bloklara bölünür) üzerinde şifreleme işlemi yapan kararlı (deterministic) algoritmalardır. Genelde blok şifrelerde blok uzunlukları 64-bit, 128-bit, 256-bit veya 512-bit olabilmektedir ve anahtar uzunlukları da Shannon'ın prensipleri [20] gereği en azından blok uzunluğu büyüklüğünde seçilmektedir. Blok şifrelerin tasarımı Shannon'ın ortaya koyduğu karıştırma (confusion) ve yayılma (diffusion) tekniklerine dayanır. Karıştırma şifre anahtarı ve şifreli metin arasındaki ilişkiyi gizlerken yayılma açık metin ve şifreli metin arasındaki ilişkiyi gizler. Diğer bir deyişle karıştırma özelliği şifreli metni kullanarak anahtarı elde etmeye çalışan saldırganı, yayılma özelliği şifreli metin istatistiklerini kullanarak açık metni elde etmeye çalışan saldırganı engellemeyi amaçlar. Blok şifrelerde karıştırma blok şifrelerin tek doğrusal olmayan parçası olan yerdeğiştirme kutuları (Substitution boxes) ya da kısaca S-kutuları ile sağlanırken yayılma doğrusal dönüşüm veya doğrusal dönüşümler yardımıyla sağlanır. Buna ek olarak blok şifreler döngü (round) adı verilen aynı işlem adımlarının arka arkaya uygulanmasından oluşur. Bu nedenle blok şifrelerde her döngüde şifreleme işleminde oluşabilecek simetrilerin ortadan kaldırılmasına yardımcı olan beyazlatma (whitening) etkisi adı da verilen farklı bir anahtar materyalinin işleme katılması gerekir. Her döngüde kullanılan birbirinden farklı anahtar materyalleri (alt anahtarlar) gizli anahtardan bir anahtar planlama algoritması (key scheduling algorithm) ile elde edilir. Kısaca bir blok şifre 3 temel katmandan oluşur:

- Doğrusal Olmayan Katman (örneğin S-kutuları),
- Yayılım Katmanı (Doğrusal Dönüşüm veya Dönüşümler),
- Anahtar Planlama Algoritması.

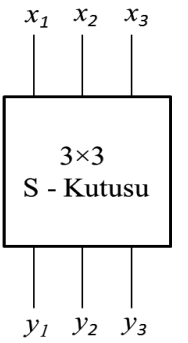
Blok şifre tasarımında iki temel tasarım mimarisi vardır [16]: Feistel Ağları ve Yerdeğiştirme ve Permütasyon Ağları (Substitution Permutation Networks) ya da kısaca SPN. Bu iki mimarideki en temel fark döngü bloğun işlenmesi sırasında ortaya çıkmaktadır. Feistel mimarisi döngü bloğun yarısını işlerken SPN mimarisi döngü bloğunun tümünü işler. SPN mimarisi bu özelliği ile daha az döngü sayısı ve aynı güvenlik seviyelerinde şifre tasarımına izin verdiğinden Feistel mimarisine karşı avantaj sağlar. Ancak Feistel mimarisine sahip bir blok şifreleme algoritmasına sadece anahtarların ters sırada uygulanması ile şifre çözme işlemi gerçekleştirilebilir. Şekil 3.1'de Feistel ve SPN mimarileri gösterilmektedir.



Şekil 3.1. Feistel ve SPN Mimarileri

3.3.1. Yer Değiştirme Kutuları (S-kutuları) için Kriptografik Test Yöntemleri

Birebir ve örten (bijective) S-kutuları birçok modern şifrenin güvenliğinin sağlanmasında önemli rol oynar ve bir blok şifrede kullanılan tek doğrusal olmayan (özellikle SPN mimarısi için) elemandır. $F_2^m \rightarrow F_2{}^m$'e ($m$-bit'ten m-bit'e ya da $m \times m$) tanımlı bir S-kutusu vektörel çıkış fonksiyonları $f_1, f_2, ..., f_m$ veya $y_1, y_2, ..., y_m$ ile temsil edilebilir. Bir blok şifre tasarımında genelde 4×4 ya da 8×8 boyutlarında S-kutuları tercih edilmektedir. Ancak bazı farklı boyutlarda uygulamaları da bir blok şifre tasarımında mümkün olabilir (Örneğin DES algoritmasında 6×4 boyutunda bir S-kutusunu kullanılmaktadır). Şekil 3.2'de 3×3 boyutunda bir S-kutusunun genel gösterimi verilmiştir.



Şekil 3.2. 3×3 Boyutunda Bir S-kutusunun Genel Gösterimi

S-kutularının elde edilmesinde/tasarımında çeşitli teknikler mevcuttur. S-kutularının tasarımında mevcut olan tekniklere örnek olarak sözde rassal (pseudo-random) üretim, sonlu cisimde üs alma, sonlu cisimde ters alma ve sezgisel (heuristic) teknikler verilebilir [15]. Bu tasarım tekniklerinden sonlu cisimde üs alma veya ters alma işlemleri ile tasarlanan S-kutuları (elde edilen S-kutusunun ve sahip olduğu çıkış boole fonksiyonlarının doğrusal olmama, cebirsel derece gibi ölçütler için bilinen maksimum ödünleşimi sağlama-

sından dolayı) popüler olmuşlardır [21]. Örneğin AES blok şifresinde 8×8 boyutunda ve sonlu cisimde ters alma yöntemi ile tasarlanmış bir S-kutusu kullanılmaktadır.

Bir S-kutusunun güvenlik ölçütleri statik ya da dinamik olarak sınıflandırılabilir [22]. Statik özellikler (örneğin doğrusal olmama ölçütü) anahtar ya da açık metin bitleri değiştirilmeden açık metin, şifreli metin ve anahtar bitleri arasındaki ilişki ile ilgilidir. Dinamik özellikler açık metin ya da anahtar bitlerinin alt kümesinde değişiklikler yapıldığında açık metin, şifreli metin ve anahtar bitlerindeki değişimlere karşılık gelir. Dinamik özelliklere örnek olarak bütünlük (completeness), çığ (avalanche), katı çığ (strict avalanche) ölçütleri gösterilebilir. Bir S-kutusunun kriptografik bir yapıda kullanılmasını belirleyen önemli kriptografik ölçütler aşağıdaki gibi verilebilir:

- Doğrusal olmama [22] [23],
- Bütünlük [24],
- Çığ [25],
- Katı çığ [26],
- Doğrusal Yaklaşım Tablosu (Linear Approximation Table) [27] [28] [29],
- Fark Dağılım Tablosu (Difference Distribution Table) [29] [30].

Bir S-kutusunun $S: F_2^n \to F_2^m$ (n-bit'ten m-bit'e ya da $n \times m$) doğrusal olmama parametresi NL_S, $A_n = \{\ a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n ; a_i \in F_2,\ 0 \le i \le n\ \}$ S-kutusunun tüm doğrusal boole fonksiyonlar kümesinin (ya da tüm giriş boole fonksiyonlarının doğrusal kombinasyonları kümesinin) $O_m = \{\ b_1 y_1 \oplus \ldots \oplus b_m y_m ;\ b_0 = 0, b_i \in F_2,\ 1 \le i \le m\ \}$ tüm çıkış fonksiyonlarının doğrusal kombinasyonları kümesine olan minimum Hamming uzaklığı olarak tanımlanır.

Not 3.3. Bir S-kutusunun doğrusal olmama özelliğinin testinde $O_m = \{\ b_1 y_1 \oplus \ldots \oplus b_m y_m ;\ b_0 = 0, b_i \in F_2,\ 1 \le i \le m\ \}$ çıkış fonksiyonlarının doğrusal kombinasyonları kümesinin

$A_n = \{ a_0 \oplus a_1 x_1 \oplus ... \oplus a_n x_n ; a_i \in F_2,\ 0 \le i \le n \}$ tüm doğrusal fonksiyonlar kümesinden $a_0 = 1$ içeren doğrusal fonksiyonlara olan Hamming uzaklıklarının elde edilmesine gerek yoktur.

Tablo 3.4. 3×3 boyutunda bir S-kutusu

Giriş (hex.)	0	1	2	3	4	5	6	7
	000	001	010	011	100	101	110	111
Çıkış (hex.)	4	5	1	2	3	6	7	0
	100	101	001	010	011	110	111	000

Örnek 3.7. Şekil 3.2'de genel gösterimi verilen 3×3 boyutunda bir S-kutusunun giriş ve çıkış değerleri Tablo 3.4'teki gibi verilsin. Bu S-kutusunun doğrusal olmama değerini elde edelim.

Verilen S-kutusunun doğrusal olmama değerinin elde edilmesi için S-kutusunun tüm giriş boole fonksiyonlarının doğrusal kombinasyonlarının kümesi (Not 3.3 de göz önüne alınarak) ve çıkış boole fonksiyonlarının doğrusal kombinasyonlarının kümesi arasındaki minimum Hamming uzaklığı elde edilmelidir. Tablo 3.5'te tüm giriş ve çıkış boole fonsiyonlar kümesinin doğrusal kombinasyonları elde edilmiştir.

Tablo 3.5. $F_2^3 \to F_2{}^3$'ye Tüm Giriş ve Çıkış Boole Fonksiyonlarının Doğrusal Kombinasyonları

Tüm Olası Doğrusal Boole Fonksiyonları	Tüm Çıkış Boole Fonksiyonlarının Doğrusal Kombinasyonları
$a_1(x) = x_1$	$o_1(y) = y_1$
$a_2(x) = x_2$	$o_2(y) = y_2$
$a_3(x) = x_3$	$o_3(y) = y_3$
$a_4(x) = x_1 \oplus x_2$	$o_4(y) = y_1 \oplus y_2$
$a_5(x) = x_1 \oplus x_3$	$o_5(y) = y_1 \oplus y_3$
$a_6(x) = x_2 \oplus x_3$	$o_6(y) = y_2 \oplus y_3$
$a_7(x) = x_1 \oplus x_2 \oplus x_3$	$o_7(y) = y_1 \oplus y_2 \oplus y_3$

Örnek olarak S-kutusunun $a_1(x) = x_1$ giriş boole fonksiyonu (doğrusal boole fonksiyonu) ile $o_6(y) = y_2 \oplus y_3$ (y_2 ve y_3 çıkış boole fonksiyonlarının doğrusal kombinasyonu) arasındaki Hamming uzaklığı $d_H(a_1, o_6) = wt(a_1(x) \oplus o_6(y)) = 6$ olarak aşağıda gösterildiği gibi elde edilebilir.

x_1	x_2	x_3	y_1	y_2	y_3	$o_6(y) = y_2 \oplus y_3$	$x_1 \oplus a_6(y)$
0	0	0	1	0	0	0	0
0	0	1	1	0	1	1	1
0	1	0	0	0	1	1	1
0	1	1	0	1	0	1	1
1	0	0	0	1	1	0	1
1	0	1	1	1	0	1	0
1	1	0	1	1	1	0	1
1	1	1	0	0	0	0	1

S-kutusunun doğrusal olmama değerinin elde edilmesi için hesaplanması gereken tüm Hamming uzaklıklarının listesi aşağıdaki gibi verilebilir. Aşağıda verilen Hamming uzaklıklarından en küçük değer 2 olduğu için S-kutusunun doğrusal olmama değeri $NL_S = 2$ olarak elde edilir.

$d_H(a_1, o_1) = 4$	$d_H(a_2, o_1) = 6$	$d_H(a_3, o_1) = 4$	$d_H(a_4, o_1) = 6$
$d_H(a_1, o_2) = 2$	$d_H(a_2, o_2) = 4$	$d_H(a_3, o_2) = 4$	$d_H(a_4, o_2) = 2$
$d_H(a_1, o_3) = 4$	$d_H(a_2, o_3) = 4$	$d_H(a_3, o_3) = 6$	$d_H(a_4, o_3) = 4$
$d_H(a_1, o_4) = 6$	$d_H(a_2, o_4) = 6$	$d_H(a_3, o_4) = 4$	$d_H(a_4, o_4) = 4$
$d_H(a_1, o_5) = 4$	$d_H(a_2, o_5) = 6$	$d_H(a_3, o_5) = 6$	$d_H(a_4, o_5) = 2$
$d_H(a_1, o_6) = 6$	$d_H(a_2, o_6) = 4$	$d_H(a_3, o_6) = 2$	$d_H(a_4, o_6) = 2$
$d_H(a_1, o_7) = 6$	$d_H(a_2, o_7) = 2$	$d_H(a_3, o_7) = 6$	$d_H(a_4, o_7) = 4$

$d_H(a_5, o_1) = 4$	$d_H(a_6, o_1) = 2$	$d_H(a_7, o_1) = 6$
$d_H(a_5, o_2) = 2$	$d_H(a_6, o_2) = 4$	$d_H(a_7, o_2) = 6$
$d_H(a_5, o_3) = 2$	$d_H(a_6, o_3) = 2$	$d_H(a_7, o_3) = 2$
$d_H(a_5, o_4) = 2$	$d_H(a_6, o_4) = 6$	$d_H(a_7, o_4) = 4$
$d_H(a_5, o_5) = 6$	$d_H(a_6, o_5) = 4$	$d_H(a_7, o_5) = 4$
$d_H(a_5, o_6) = 4$	$d_H(a_6, o_6) = 2$	$d_H(a_7, o_6) = 4$
$d_H(a_5, o_7) = 4$	$d_H(a_6, o_7) = 4$	$d_H(a_7, o_7) = 6$

Doğrusal Yaklaşım Tablosu (Lineer Approximation Table-LAT) doğrusal kriptoanalize karşı S-kutularının güvenliğinin ölçülmesinde çok önemli bir test ölçütüdür ve doğrusal olmama ölçütü ile yakından ilişkilidir. Verilen bir S-kutusu $S: F_2^n \to F_2^m$ için Γ_A. satır ve Γ_B. sütun $LAT(\Gamma_A, \Gamma_B)$ aşağıdaki gibi tanımlanabilir:

$$LAT(\Gamma_A, \Gamma_B) = \#\{x \in F_2^n | \Gamma_A \bullet x = \Gamma_B \bullet S(x)\} - 2^{n-1}.$$

Verilen ifadede x S-kutusunun giriş bitlerini, $S(x)$ S-kutusunun çıkış bitlerini $\Gamma_A \neq 0$ olmak üzere $\Gamma_A \in F_2^n$, $\Gamma_B \in F_2^m$ sırasıyla giriş ve çıkış maskelerini ifade etmektedir. Buna ek olarak elde edilen LAT tablosu $2^n \times 2^m$ boyutundadır. Doğrusal kriptoanalizin karmaşıklığı en büyük LAT girişinin ($\max_{\Gamma_A, \Gamma_B} |\mathrm{LAT_S}(\Gamma_A, \Gamma_B)|$) genişliğine (mutlak değerine) bağlıdır. Şifreleme algoritması için doğrusal yaklaşım tablosunda bulunan maksimum mutlak değerin küçük olması doğrusal kriptoanaliz saldırısının başarımını zorlaştırmaktadır. Buna ek olarak en büyük mutlak LAT girişi bir S-kutusunun doğrusal olmama değeri NL_S'i (aşağıda gösterildiği gibi) elde etmede kullanılabilir:

$$NL_S = 2^{n-1} - \max_{\Gamma_A, \Gamma_B} |LAT_S(\Gamma_A, \Gamma_B)|.$$

Tablo 3.6. PRESENT [31] Hafif Sıklet Blok Şifresinde Kullanılan 4×4 boyutunda S-kutusu

Giriş (hex.)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Çıkış (hex.)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Örnek 3.8. Tablo 3.6'da verilen ve PRESENT hafif sıklet blok şifresinde kullanılan 4×4 boyutundaki S-kutusunun $LAT(5, \mathrm{A})$ değerinin elde edilişini, LAT tablosunu ve LAT tablosunu kullanarak S-kutusunun doğrusal olmama değerini elde edelim. Not: Hexadecimal 5 ve A değerleri sırasıyla giriş maskesi 0101 ve çıkış maskesi 1010 ikili değerlerini temsil etmektedir.

$LAT(5, \mathrm{A})$ değerinin elde edilişi aşağıdaki tablo yardımıyla gösterilebilir:

(0101) • (0000) = (1010) • (1100)	→	0≠1
(0101) • (0001) = (1010) • (0101)	→	1≠0
(0101) • (0010) = (1010) • (0110)	→	0≠1
(0101) • (0011) = (1010) • (1011)	→	1≠0
(0101) • (0100) = (1010) • (1001)	→	1=1 *
(0101) • (0101) = (1010) • (0000)	→	0=0 *
(0101) • (0110) = (1010) • (1010)	→	1≠0
(0101) • (0111) = (1010) • (1101)	→	0≠1
(0101) • (1000) = (1010) • (0011)	→	0≠1
(0101) • (1001) = (1010) • (1110)	→	1≠0
(0101) • (1010) = (1010) • (1111)	→	0=0 *
(0101) • (1011) = (1010) • (1000)	→	1=1 *
(0101) • (1100) = (1010) • (0100)	→	1≠0
(0101) • (1101) = (1010) • (0111)	→	0≠1
(0101) • (1110) = (1010) • (0001)	→	1≠0
(0101) • (1111) = (1010) • (0010)	→	0≠1

Yukarıdaki tablodan $LAT(5, \mathrm{A})$ için eşitliği sağlayan (* ile işaretlenmiş olanlar) 4 değer bulunmaktadır. Dolayısıyla $LAT(\Gamma_A, \Gamma_B)$ tanımı gereği $LAT(5,\mathrm{A}) = 4 - 2^{4-1} = 4 - 8 = -4$ şeklinde elde edilir. Tablo 3.7'de S-kutusunun LAT tablosu verilmiştir. S-kutusunun doğrusal olmama değeri NL_S, tüm LAT tablosu elemanlarının en büyük mutlak değeri göz önüne alınarak $NL_S = 2^{4-1} - 4 = 4$ şeklinde elde edilebilir.

Tablo 3.7. PRESENT Hafif Sıklet Blok Şifresinde Kullanılan 4×4 boyutunda S-kutusunun Doğrusal Yaklaşım Tablosu

		Çıkış Maskesi (Γ_B)															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Giriş Maskesi (Γ_A)	**0**	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	-4	0	-4	0	0	0	0	0	-4	0	4
	2	0	0	2	2	-2	-2	0	0	2	-2	0	4	0	4	-2	2
	3	0	0	2	2	2	-2	-4	0	-2	2	-4	0	0	0	-2	-2
	4	0	0	-2	2	-2	-2	0	4	-2	-2	0	-4	0	0	-2	2
	5	0	0	-2	2	-2	2	0	0	2	2	-4	0	4	0	2	2
	6	0	0	0	-4	0	0	-4	0	0	-4	0	0	4	0	0	0
	7	0	0	0	4	4	0	0	0	0	-4	0	0	0	0	4	0
	8	0	0	2	-2	0	0	-2	2	-2	2	0	0	-2	2	4	4
	9	0	4	-2	-2	0	0	2	-2	-2	-2	-4	0	-2	2	0	0
	A	0	0	4	0	2	2	2	-2	0	0	0	-4	2	2	-2	2
	B	0	-4	0	0	-2	-2	2	-2	-4	0	0	0	2	2	2	-2
	C	0	0	0	0	-2	-2	-2	-2	4	0	0	-4	-2	2	2	-2
	D	0	4	4	0	-2	-2	2	2	0	0	0	0	2	-2	2	-2
	E	0	0	2	2	-4	4	-2	-2	-2	-2	0	0	-2	-2	0	0
	F	0	4	-2	2	0	0	-2	-2	-2	2	4	0	2	2	0	0

Kriptografik bir yapının test edilmesinde kullanılan ve bu bölümde sunulacak dinamik özellikler sırasıyla bütünlük, çığ ve katı çığ ölçütleridir. Örneğin çığ veye katı çığ ölçütleri bir anahtar planlama algoritmasının kriptografik gücünün incelenmesinde de kullanılabilir. Bu ölçütler dışında bir S-kutusunun test edilmesinde kullanılan Fark Dağılım Tablosu (Difference Distribution Table) ölçütü S-kutusunun diferansiyel kriptoanalize karşı dayanıklılığın değerlendirilmesinde kullanılmaktadır.

Kam ve Davida'nın tanımladığı bütünlük [24], Feistel tarafından tanımlanan çığ [25], Webster ve Tavares tarafından (bütünlük ve çığ ölçütleri birleştirilerek) tanımlanan katı çığ [26] ölçütleri birbirleriyle yakından ilgili ölçütlerdir. Bütünlük, çığ ve katı çığ ölçütleri kabaca kriptografik yapının (örneğin S-kutusu) giriş bitlerinden birinin değişiminde sırasıyla çıkış bitlerinin değişmesi gerekliliğini, çıkış bitlerinin tam olarak yarısının değişmesi gerekliliğini ve her çıkış bitinin tam olarak yarısının değişmesi gerekliliğini tanımlar.

Bir $f\colon F_2^n \to F_2^m$ kriptografik fonksiyonunun (n-bit giriş ve m-bit çıkış) bütünlük ölçütünü sağlayabilmesi için en az bir tane $x \in F_2^n$ için $i \in \{1,2,..., n\}$ ve $j \in \{1,2,..., m\}$ olmak üzere $f(x)$ ve $f(x \oplus \Delta x_i)$'in bit j'de farklılaşması gerekir. Diğer bir deyişle her çıkış bitinin giriş bitlerinin tümüne bağlı olması beklenir. Bu bağlamda fonksiyon f'nin çığ (avalanche) vektörü aşağıdaki gibi ifade edilebilir [22] [23] [28]:

$$\Delta y^{\Delta x_i} = f(x) \oplus f(x \oplus \Delta x_i) = [a_1^{\Delta x_i} a_2^{\Delta x_i} \ldots a_m^{\Delta x_i}],\ a_j^{\Delta x_i} \in F_2$$

$\Delta y^{\Delta x_i}$, çığ vektörü, giriş vektöründen sadece bir biti (i. bit) değiştirilerek elde edilmiş fark şeridir. Çığ vektöründeki toplam değişim aşağıdaki gibi ifade edilebilir:

$$wt\,(a_j^{\Delta x_i}) = \sum_{her\ x \in F_2^n\ için} a_j^{\Delta x_i}$$

Çığ vektöründeki toplam değişimin aralığı $0 \le wt(a_j^{\Delta x_i}) \le 2^n$ şeklindedir ve maksimum 2^n'dir. Buna ek olarak fark vektörü Δx_i aşağıdaki gibi ifade edilebilir:

$$\begin{aligned} \Delta x_1 &= (1,0,0,..,0), \\ \Delta x_2 &= (0,1,0,..,0), \\ &\vdots \\ \Delta x_n &= (0,0,0,..,1). \end{aligned}$$

Verilen tanımlardan çığ vektöründeki toplam değişim 0 ($wt(a_j^{\Delta x_i}) = 0$) ise bütünlük ölçütü sağlanmamış olmaktadır. Çığ vektöründeki toplam değişimin 2^n ($wt(a_j^{\Delta x_i}) = 2^n$) olduğu durumda ise giriş biti i'nin değili alındığında çıkış biti j'nin bundan doğrudan etkilendiği anlamına gelmektedir. Bu toplam değişim miktarı da istenmeyen bir özellik olarak karşımıza çıkar. Sonuçta $\frac{1}{2^n} wt(a_j^{\Delta x_i})$ ifadesi [0,1] aralığında değerler alır. Eğer kriptografik fonksiyon bütün değilse $\frac{1}{2^n} wt(a_j^{\Delta x_i})$ ifadesi 0 ya da 1 olacaktır.

Çığ ölçütü, bir $f: F_2^n \to F_2^m$ kriptografik fonksiyonu için giriş bitinin bir biti değiştiğinde çıkış bitlerinin yarısının değişmesi anlamına gelmektir. Bu bağlamda fonksiyon f'nin çığ ölçütünü sağlaması için $i \in \{1,2,..., n\}$ ve $j \in \{1,2,..., m\}$ giriş ve çıkış vektör bitleri olmak üzere tüm i değerleri (giriş bitleri) için

$$\frac{1}{2^n} \sum_{j=1}^{m} wt(a_j^{\Delta X_i}) = \frac{m}{2}$$

ifadesini sağlamalıdır. Verilen ifade tekrar düzenlenirse çığ parametresi $k_A(i)$ aşağıdaki gibi elde edilebilir.

$$k_A(i) = \frac{1}{m.2^n} \sum_{j=1}^{m} wt(a_j^{\Delta X_i}) = \frac{1}{2}$$

Çığ parametresi $k_A(i)$, herhangi bir i değeri için $\frac{1}{2}$ değerinden farklı bir değer alırsa kriptografik fonksiyon çığ ölçütünü sağlamaz.

Katı çığ ölçütü, bir $f: F_2^n \to F_2^m$ kriptografik fonksiyonu için herhangi bir giriş biti değiştiğinde herhangi bir çıkış bitinin kesinlikle yarısının değişmesi anlamına gelmektedir. Bu bağlamda fonksiyon f'nin katı çığ ölçütünü sağlaması için $i \in \{1,2,..., n\}$ ve $j \in \{1,2,..., m\}$ giriş ve çıkış vektör bitleri olmak üzere tüm i ve j değerleri için aşağıdaki ifadeyi sağlaması gerekir:

$$\frac{1}{2^n} wt(a_j^{\Delta X_i}) = \frac{1}{2}$$

Dolayısıyla katı çığ parametresi $k_{SAC}(i, j)$ aşağıdaki şekilde elde edilebilir:

$$k_{SAC}(i, j) = \frac{1}{2^n} wt(a_j^{\Delta x_i})$$

Yukarıda verilen $k_{SAC}(i,j)$ parametresi [0,1] aralığında değerler alır ve eğer herhangi bir (i , j) kombinasyonu için $\frac{1}{2}$ değerinden farklı ise o zaman fonksiyon katı çığ ölçütünü sağlamaz.

Örnek 3.9. Tablo 3.4'de verilen 3×3 S-kutusu için bütünlük, çığ ve katı çığ ölçütlerini sağlayıp sağlamadığını elde edelim.

Verilen S-kutusu 3×3 boyutunda olduğu için $n = m = 3$'tür ve fark vektörü Δx_i, $\Delta x_1 = (1,0,0)$, $\Delta x_2 = (0,1,0)$ ve $\Delta x_3 = (0,0,1)$ şeklindedir. Aşağıdaki tabloda 3×3 boyutunda ki S-kutusu ve tüm x giriş değerleri için $\Delta S^{\Delta x_1} = S(x) \oplus S(x \oplus \Delta x_1) = (a_1^{\Delta x_1}, a_2^{\Delta x_1}, a_3^{\Delta x_1})$ elde edilmektedir.

x	Δx_1	$x \oplus \Delta x_1$	$y = S(x)$	$S(x \oplus \Delta x_1)$	$\Delta S^{\Delta x_1} = S(x) \oplus S(x \oplus \Delta x_1)$ $(a_1^{\Delta x_1}, a_2^{\Delta x_1}, a_3^{\Delta x_1})$
000	100	100	100	011	111
001	100	101	101	110	011
010	100	110	001	111	110
011	100	111	010	000	010
100	100	000	011	100	111
101	100	001	110	101	011
110	100	010	111	001	110
111	100	011	000	010	010

Yukarıdaki tablodan $wt(a_1^{\Delta x_1}) = 4$, $wt(a_2^{\Delta x_1}) = 8$ ve $wt(a_3^{\Delta x_1}) = 4$ olarak elde edilir. Aşağıdaki tabloda 3×3 boyutunda ki S-kutusu ve tüm x giriş değerleri için $\Delta S^{\Delta x_2} = S(x) \oplus S(x \oplus \Delta x_2) = (a_1^{\Delta x_2}, a_2^{\Delta x_2}, a_3^{\Delta x_2})$ elde edilmektedir.

x	Δx_2	$x \oplus \Delta x_2$	$y = S(x)$	$S(x \oplus \Delta x_2)$	$\Delta S^{\Delta x_2} = S(x) \oplus S(x \oplus \Delta x_2)$ $(a_1^{\Delta x_2}, a_2^{\Delta x_2}, a_3^{\Delta x_2})$
000	010	010	100	001	101
001	010	011	101	010	111
010	010	000	001	100	101
011	010	001	010	101	111
100	010	110	011	111	100
101	010	111	110	000	110
110	010	100	111	011	100
111	010	101	000	110	110

Yukarıdaki tablodan $wt(a_1^{\Delta x_2}) = 8$, $wt(a_2^{\Delta x_2}) = 4$ ve $wt(a_3^{\Delta x_2}) = 4$ olarak elde edilir. Aşağıdaki tabloda 3×3 boyutunda ki S-kutusu ve tüm x giriş değerleri için $\Delta S^{\Delta x_3} = S(x) \oplus S(x \oplus \Delta x_3) = (a_1^{\Delta x_3}, a_2{}^{\Delta x_3}, a_3^{\Delta x_3})$ elde edilmektedir.

x	Δx_3	$x \oplus \Delta x_3$	$y = S(x)$	$S(x \oplus \Delta x_3)$	$\Delta S^{\Delta x_3} = S(x) \oplus S(x \oplus \Delta x_3)$ $(a_1^{\Delta x_3}, a_2{}^{\Delta x_3}, a_3^{\Delta x_3})$
000	001	001	100	101	001
001	001	000	101	100	001
010	001	011	001	010	011
011	001	010	010	001	011
100	001	101	011	110	101
101	001	100	110	011	101
110	001	111	111	000	111
111	001	110	000	111	111

Yukarıdaki tablodan $wt(a_1^{\Delta x_3}) = 4$, $wt(a_2^{\Delta x_3}) = 4$ ve $wt(a_3^{\Delta x_3}) = 8$ olarak elde edilir. Elde edilen sonuçlardan çığ paremetreleri ($n = m = 3$ olduğu için) aşağıdaki gibi elde edilebilir:

$$k_A(1) = \frac{1}{n.2^n}\sum_{j=1}^{n} wt(a_j^{\Delta X_1}) = \frac{wt(a_1^{\Delta X_1}) + wt(a_2^{\Delta X_1}) + wt(a_3^{\Delta X_1})}{3.2^3} = \frac{16}{24} = \frac{2}{3}$$

$$k_A(2) = \frac{1}{n.2^n}\sum_{j=1}^{n} wt(a_j^{\Delta X_1}) = \frac{wt(a_1^{\Delta X_2}) + wt(a_2^{\Delta X_2}) + wt(a_3^{\Delta X_3})}{3.2^3} = \frac{16}{24} = \frac{2}{3}$$

$$k_A(3) = \frac{1}{n.2^n}\sum_{j=1}^{n} wt(a_j^{\Delta X_1}) = \frac{wt(a_1^{\Delta X_3}) + wt(a_2^{\Delta X_3}) + wt(a_3^{\Delta X_3})}{3.2^3} = \frac{16}{24} = \frac{2}{3}$$

Diğer yandan S-kutusunun katı çığ parametereleri aşağıdaki gibi elde edilebilir:

$$k_{SAC}(1,1) = \frac{1}{2^n} wt(a_1^{\Delta x_1}) = \frac{4}{8} = \frac{1}{2},$$

$$k_{SAC}(1,2) = \frac{1}{2^n} wt(a_2^{\Delta x_1}) = \frac{8}{8} = 1,$$

$$k_{SAC}(1,3) = \frac{1}{2^n} wt(a_3^{\Delta x_1}) = \frac{4}{8} = \frac{1}{2},$$

$$k_{SAC}(2,1) = \frac{1}{2^n} wt(a_1^{\Delta x_2}) = \frac{8}{8} = 1,$$

$$k_{SAC}(2,2) = \frac{1}{2^n} wt(a_2^{\Delta x_2}) = \frac{4}{8} = \frac{1}{2},$$

$$k_{SAC}(2,3) = \frac{1}{2^n} wt(a_3^{\Delta x_2}) = \frac{4}{8} = \frac{1}{2},$$

$$k_{SAC}(3,1) = \frac{1}{2^n} wt(a_1^{\Delta x_3}) = \frac{4}{8} = \frac{1}{2},$$

$$k_{SAC}(3,2) = \frac{1}{2^n} wt(a_2^{\Delta x_3}) = \frac{4}{8} = \frac{1}{2},$$

$$k_{SAC}(3,3) = \frac{1}{2^n} wt(a_3^{\Delta x_3}) = \frac{8}{8} = 1.$$

Sonuç olarak S-kutusu, çığ ve katı çığ paremetrelerinde $\frac{1}{2}$ değerinden farklı değerler bulunduğu için bu ölçütleri sağlamaz. Buna ek olarak S-kutusunun katı çığ parametreleri içerisinde 1 değerine sahip parametreler olduğu için verilen S-kutusu bütünlük ölçütünü de sağlamaz.

Bir S-kutusu için tanımlanan Fark Dağılım Tablosu (veya XOR dağılım tablosu) bir blok şifrenin diferansiyel kriptoanalize karşı dayanıklılığı ile ilgili bilgi veren önemli bir ölçüttür. Bir $n \times m$ boyutunda S-kutusu için Fark Dağılım Tablosu $2^n \times 2^m$ boyutlu matrise denk düşer. Bir S-kutusu $S: F_2^n \rightarrow F_2^m$ (n-bit giriş ve m-bit çıkışa sahip bir S-kutusu) ve verilen herhangi $a \in F_2^n, a \neq 0$ ve $b \in F_2^m$ için $XOR\ (a,b),\ S(x) \oplus S(x \oplus a) = b$ denklemindeki b değerlerinin sayısını tanımlar ve aşağıdaki gibi gösterilebilir:

$$XOR(a,b) = \#\left\{x \in F_2^n \mid S(x) \oplus S(x \oplus a) = b\right\}.$$

Yukarıda verilen ifade de a ve b değerleri sırasıyla giriş farkı ve çıkış farkı olarak isimlendirilir. Diferansiyel kriptoanalize karşı dayanıklı bir S-kutusunun Fark Dağılım Tablosundaki girişlerin büyük değerlere sahip olmaması gerekir.

Örnek 3.10. Tablo 3.5'te verilen ve PRESENT hafif sıklet blok şifresinde kullanılan 4×4 boyutundaki S-kutusunun $XOR(2,5)$ değerinin elde edilişini ve Fark Dağılım Tablosunu elde edelim. Not: Hexadecimal 2 ve 5 değerleri sırasıyla giriş farkı 0010 ve çıkış farkı 0101 ikili değerlerini temsil etmektedir.

PRESENT S-kutusu için $XOR(2,5)$ değerlerinin elde edilişi aşağıdaki tablo yardımıyla gösterilebilir:

S(0)	⊕	S(0⊕2)	=	S(0)	⊕	S(2)	=	C	⊕	6	=	A	
S(1)	⊕	S(1⊕2)	=	S(1)	⊕	S(3)	=	5	⊕	B	=	E	
S(2)	⊕	S(2⊕2)	=	S(2)	⊕	S(0)	=	6	⊕	C	=	A	
S(3)	⊕	S(3⊕2)	=	S(3)	⊕	S(1)	=	B	⊕	5	=	E	
S(4)	⊕	S(4⊕2)	=	S(4)	⊕	S(6)	=	9	⊕	A	=	3	
S(5)	⊕	S(5⊕2)	=	S(5)	⊕	S(7)	=	0	⊕	D	=	D	
S(6)	⊕	S(6⊕2)	=	S(6)	⊕	S(4)	=	A	⊕	9	=	3	
S(7)	⊕	S(7⊕2)	=	S(7)	⊕	S(5)	=	D	⊕	0	=	D	
S(8)	⊕	S(8⊕2)	=	S(8)	⊕	S(A)	=	3	⊕	F	=	C	
S(9)	⊕	S(9⊕2)	=	S(9)	⊕	S(B)	=	E	⊕	8	=	6	
S(A)	⊕	S(A⊕2)	=	S(A)	⊕	S(8)	=	F	⊕	3	=	C	
S(B)	⊕	S(B⊕2)	=	S(B)	⊕	S(9)	=	8	⊕	E	=	6	
S(C)	⊕	S(C⊕2)	=	S(C)	⊕	S(E)	=	4	⊕	1	=	5	*
S(D)	⊕	S(D⊕2)	=	S(D)	⊕	S(F)	=	7	⊕	2	=	5	*
S(E)	⊕	S(E⊕2)	=	S(E)	⊕	S(C)	=	1	⊕	4	=	5	*
S(F)	⊕	S(F⊕2)	=	S(F)	⊕	S(D)	=	2	⊕	7	=	5	*

Yukarıda verilen tablo yardımıyla $XOR(2,5)$ için eşitliği sağlayan (* ile işaretlenmiş olanlar) 4 değer olduğu elde edilir. Tablo 3.8'de S-kutusunun Fark Dağılım Tablosu verilmiştir.

Tablo 3.8. PRESENT Hafif Sıklet Blok Şifresinde Kullanılan 4×4 boyutunda S-kutusunun Fark Dağılım Tablosu

		Çıkış Farkı (b)															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Giriş Farkı (a)	**0**	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
	2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
	3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
	4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
	5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
	6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
	7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
	8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
	9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
	A	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
	B	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
	C	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
	D	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
	E	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
	F	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Bu bölümde ayrıntılı incelenen kriptografik ölçütler dışında Bit Bağımsızlık (Bit Independence) [26], MOSAC (Maximum Order SAC) [32] ve MOBIC (Maximum Order BIC) [32] ölçütleri kriptografik bir yapının değerlendirilmesinde kullanılan diğer ölçütlerdir. Bununla beraber özellikle sonlu cisimde ters haritalama veya üs

haritalama teknikleri ile geliştirilen ve iyi kriptografik özellikleri olan S-kutularının (Örneğin AES S-kutusu) istenmeyen bir özellik olan doğrusal artıklık (linear redundancy) özelliğine sahip olduğu [15] çalışmasında gösterilmiştir. Bunun nedeni bu tip S-kutularının çıkış boole fonksiyonlarının aynı denklik sınıfına ait olmasıdır.

3.3.2. Doğrusal Dönüşümler için Kriptografik Test Yöntemleri

Doğrusal dönüşümler sabit uzunluktaki bir bloğu giriş alarak sabit uzunlukta bir çıkış bloğuna dönüştüren ve bu sayede bloğun doğrusal olarak karıştırılmasını sağlayan kriptografik bileşenlerdir. Doğrusal dönüşüm veya dönüşümlerin kullanılması ile kriptografik yapıların çığ özelliklerinin geliştirilmesi ve bu yapılarda gerekli yayılımın sağlanması amaçlanmaktadır [33] [34]. Diğer yandan bir blok şifrenin döngü fonksiyonunda doğrusal olmayan yapılar (örneğin S-kutuları) ile beraber kullanılarak şifrenin doğrusal ve diferansiyel kriptoanalize karşı dayanıklı olmasında da önemli rol üstlenirler.

Literatürde blok şifrelerin tasarımında kullanılan SPN ve Feistel mimarilerinin döngü fonksiyonlarında genellikle maksimum uzaklıkta ikili doğrusal (Maximum Distance Binary Linear-MDBL) ve maksimum uzaklıkta ayrılabilebilen (Maximum Distance Separable-MDS) matrisler doğrusal dönüşüm katmanı veya doğrusal dönüşüm katmanının ana bileşeni olarak kullanılmaktadır. Örneğin ARIA [35] blok şifresinde 16×16 boyutunda involutif ($A = A^{-1}$) bir MDBL matris tüm döngü fonksiyonunda doğrusal dönüşüm katmanı olarak kullanılırken AES blok şifresinde 4×4 boyutunda dairesel bir MDS matris (Sütunları Karıştırma Dönüşümü-MixColumns) AES'in döngü fonksiyonunda doğrusal dönüşüm katmanının ana bileşeni olarak kullanılmaktadır. Dolayısıyla AES blok şifresinin doğrusal dönüşüm katmanı Satırları Öteleme (ShiftRows) ve 4 tane MixColumns dönüşümü ile beraber düşünülmelidir. Ayrıca ARIA blok şifresinde kullanılan 16×16 boyutunda involutif ikili matris 16 byte (128-bit) değeri giriş alarak 16 byte değer çıkış üreten bir doğrusal dönüşümdür. AES blok şifresinde kullanılan 4×4 boyutunda ki MDS matris ise 4 byte (32-bit) değeri giriş olarak alan ve 4 byte çıkış üreten bir doğrusal dönüşümdür.

MDS matrisler, MDS kodlardan elde edilirler. Bir MDS matris, üreteç matrisi $[I,A]$ olan bir $[n,k,d]$ parametreli kodun $d=n-k+1$ Singleton sınırını karşılayan A matrisidir. MDS matrisler maksimum dal sayısı (branch number) özelliğine sahiptirler: $k\times k$ boyutundaki bir MDS matrisin dal sayısı $k+1$'dir [36]. Bu özellik, bir blok şifrede maksimum yayılımın sağlanmasına yardımcı olan en önemli kriptografik özelliktir ve $k\times k$ boyutundaki bir $M:(F_2^m)^k \to (F_2^m)^k$ matrisinin dal sayısı aşağıdaki tanımlanabilir:

$$\beta = \min\left\{wt(x) + wt(M \cdot x^T) \mid x \in (F_2^m)^k, x \neq 0\right\}$$

Verilen ifadede k aynı zamanda doğrusal dönüşüme giriş olan S-kutularının sayısını temsil etmektedir ve her S-kutusunun giriş ve çıkışının genişliği m-bittir. Yine yukarıda verilen bir M matrisi için dal sayısı tanımı, diferansiyel dal sayısı olarakta ifade edilebilir. Verilen bir matris M'nin transposunun (M^T) yukarıdaki ifade de M ile yer değiştirilmesi ile doğrusal dal sayısı tanımı elde edilebilir. MDS matrislerde diferansiyel ve doğrusal dal sayısı değerleri aynıdır. Dolayısıyla bir MDS matrisin diferansiyel dal sayısı elde edildiğinde doğrusal dal sayısı değerinin elde edilmesine gerek kalmaz. Ancak ikili bir matrisin diferansiyel ve doğrusal dal sayıları birbirinden farklılık gösterebilir. Dolayısıyla kriptografik yapıda kullanılmadan önce ikili bir matrisin hem diferansiyel hem de doğrusal dal sayılarının testi gereklidir.

Not 3.4. Diferansiyel dal sayısı bir blok şifnresinin diferansiyel kriptoanalize karşı dayanıklılığının, doğrusal dal sayısı ise doğrusal kriptoanalize karşı dayanıklılığının değerlendirilmesinde kullanılan iki önemli ölçüttür.

Sonlu cisim elemanlarına sahip $k\times k$ boyutunda bir matris M'nin MDS özelliğine sahip olabilmesi için tanımlı olunan sonlu cisimde tüm kare alt matrislerinin determinantının 0'dan farklı olması gerekir. Bu özellik gereği herhangi bir MDS matrisin elemanı 0 olamaz. Bir matrisin MDS matris olup olmadığının testinde tüm alt kare matrislerinin determinantları elde edilerek bunlardan herhangi birinin 0 olup olmadığını denetleyen bir yazılım geliştirilebilir. Diğer

yandan bu özelliğin testi için MAGMA hesaplayıcı kolaylıkla kullanılabilir [37] [38].

Örnek 3.11. AES blok şifresinde kullanılan sonlu cisim $F_{2^8}/11B$ elemanlarına sahip dairesel matrisin

$$M_1 = circ(02, 03, 01, 01) = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$ dal sayısı değeri 5

olacak şekilde aşağıda verilen MAGMA kodu ve MAGMA hesaplayıcı yardımıyla elde edilebilir. Not: $F_{2^8}/11B$ sonlu cismi F_{2^8} cisminin hexadecimal $11B$ diğer bir deyişle $x^8 + x^4 + x^3 + x + 1$ indirgenemez polinomu ile tanımlı olduğunu ifade etmektedir ve F_{2^8} sonlu cisminde hexadecimal 02 değeri polinomsal gösterimle x elemanına, hexadecimal 03 değeri ise x+1 elemanına karşılık gelmektedir.


```
P<z> := PolynomialRing(GF(2));
p := z^8 +z^4+z^3+z+1;
F<x> := ext <GF(2) | p >;
M1:=Matrix(F,4,4,[
x,x+1,1,1,
1,x,x+1,1,
1,1,x,x+1,
x+1,1,1,x
]);
I := IdentityMatrix(F,4);
C:= LinearCode(HorizontalJoin(I,M1));
MinimumWeight(C);
```

Örnekte verilen ve AES şifresinde kullanılan MDS matrisin MDS özelliğinin döngü fonksiyonundaki etkisi şu şekilde de açıklanabilir: 4×4 boyutunda giriş elemanları byte değerler (ya da elemanları sonlu cisim F_{2^8} /$11B$ olan) olan MDS matrisin bir bitindeki (dolayısıyla 1 byte'ındaki değişim) çıkıştaki minimum 4 byte'ın değişimine, girişteki 2 byte'ındaki değişim çıkıştaki minimum 3 byte'ın değişimine, girişteki 3 byte'ındaki değişim çıkıştaki minimum 2 byte'ın değişimine, girişteki 4 byte'ındaki değişim çıkışındaki minimum 1 byte'ın değişimine neden olmaktadır. Bu da toplamda giriş ve çıkıştaki 8 byte'tan minimum 5 byte'ın etkileneceği anlamına gelmektedir. AES blok şifresinde doğrusal dönüşümün önemli diğer parçası ShiftRows dönüşümünün etkisi ile beraber şifrenin 4 döngü sonucunda minimum 25 aktif S-kutusuna (herhangi bir açık metindeki bit değişimden etkilenen S-kutusu sayısı) sahip olması anlamına gelir. β örnekte verilen dairesel MDS matrisin dal sayısı olmak üzere, bu etkiye β^2 etkisi de denmektedir. Sonuçta AES blok şifresinde kullanılan S-kutularının kriptografik özellikleri ile beraber AES blok şifresine 4 döngüden sonra yapılacak doğrusal ve diferansiyel saldırılar etkisiz hale gelmektedir (Örnek 3.14 ve Örnek 3.15).

Literatürde MDS matrislerin elde edilmesinde kullanılan çeşitli teknikler mevcuttur. Bu tekniklerden Cauchy matrisler [39] ve Vandermonde matrisler [40] kullanılarak doğrudan MDS matrisler elde edilebilir. Diğer yandan dairesel ve Hadamard matris gibi matris türleri kullanılarak arama tabanlı teknikler ile MDS matrisler de elde edilebilmektedir. MDS matris elde edilmesinde bu özel matris türlerinin kullanılmasının temel nedenleri sırasıyla:

- arama ile rassal aramaya göre daha yüksek olasılıkla MDS matris elde edilmesi,
- yazılım ve donanım uygulamaları için uygun maliyetli MDS matrislerinin elde edilmesi

şeklinde verilebilir. Bununla beraber Hadamard matrisler özellikle involutif MDS matrislerin elde edilmesinde kullanılmaktadır ve bir blok şifre tasarımında involutif doğrusal dönüşümlerin kullanılması şifreleme ve şifre çözme işlemelerinin birbirine yakın maliyette

yapılmasına olanak sağlamaktadır. Bu özel matris formlarına ek olarak [41] çalışmasında Hadamard matris genelleştirilerek Genel Hadamard matris (GHadamard) özel formu tanıtılmıştır. Bu form (melez yöntem) sayesinde çok sayıda involutif ve MDS matris özellikle donanım uygulamaları hedef alınarak üretilmiştir.

MDBL matrislerin üretilmesi ile ilgili çeşitli tekniklere [34][42][43][44][45] çalışmalarından ulaşılabilir. Bu tür matrislerin bir blok şifrede kullanılmasının temel nedeni sadece XOR işlemli olarak uygulanabilir olmasıdır. Bu avantajına karşın MDBL matrislerin aynı boyuttaki maksimum dal sayısı değerleri MDS matrislerin sahip olduğı değerlere göre daha düşüktür. Örneğin 4×4 ve 8×8 boyutundaki bir MDS matrisin maksimum dal sayısı değerleri sırasıyla 5 ve 9 iken aynı boyutlardaki bir MDBL matrisin maksimum dal sayısı değerleri sırasıyla 4 ve 5'tir. Buna ek olarak $k \times k$ boyutundaki bir MDBL matrisin $k > 18$ için maksimum dal sayısı tam olarak bilinmemektedir ve $k > 18$ için $k \times k$ boyutunda bir MDBL matris için maksimum erişilebilir dal sayısı değerleri mevcuttur [45].

Örnek 3.12. 4×4 boyutunda $M_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ ikili matrisinin dal sayısı 4 olduğu aşağıda verilen MAGMA kodu ve MAGMA hesaplayıcı yardımıyla elde edilebilir.

```
M2:=Matrix(GF(2),4,4,[
0,1,1,1,
1,0,1,1,
1,1,0,1,
1,1,1,0]);
I := IdentityMatrix(GF(2),4);
C:= LinearCode(HorizontalJoin(I,M2));
MinimumWeight(C);
```

Dal sayısı ölçütüne ek olarak doğrusal dönüşümler için diğer bir ölçüt, bir doğrusal dönüşümdeki sabit nokta sayısıdır. Bu ölçüt, bir doğrusal dönüşümün çıkış bloğunu üretirken giriş bloğunu ne kadar etkin bir şekilde değiştirdiği ile ilişkilidir. Rassal bir doğrusal dönüşümde umulan sabit nokta sayısı değeri 1'dir ve bu değerin aşılması doğrusal dönüşümün zayıf yayılımının bir göstergesi olarak kabul edilir. Çünkü doğrusal dönüşüm sabit noktalarda çıkış bloğu üretirken giriş bloğunundaki bitleri çıkışa değiştirmeden aktarır. Bu ölçüt ile ilgili detaylı bilgi [33] çalışmasından elde edilebilir. Bu ölçütlere ek olarak bir MDS matrisin donanım uygulaması ile ilgili yeni bir ölçüt XOR sayısı (XOR count) [46] çalışmasında verilmiştir. Bu ölçüt hafif sıklet MDS matrislerin üretilmesi ile ilgili bir ölçüttür.

3.3.3 Anahtar Planlama Algoritmaları için Kriptografik Test Yöntemleri

Anahtar planlama algoritmaları, bir blok şifrenin her döngü fonksiyonunda kullanılan birbirinden farklı alt anahtarların elde edilmesini sağlayan algoritmalardır. Birbirinden farklı alt anahtarlar, gizli anahtar ve anahtar planlama algoritması (key scheduling algorithm) ile elde edilirler. Anahtar planlama algoritmaları, genellikle blok şifrelerin döngü fonksiyonlarında kullanılan kriptografik yapıların kullanılması ile tasarlanırlar ve bu algoritmalar için maliyeti uygun tasarımlar tercih edilir. Tasarımı iyi yapılmayan anahtar planlama algoritmaları ilişkili anahtar saldırıları (Related Key Attacks) gibi saldırılara neden olabilmektedir [47]. Buna ek olarak blok şifreleme algoritmalarının birçoğunda kullanılan anahtar planlama algoritmaları çeşitli kriptanalitik saldırılarda yardımcı rol üstlenebilmektedir. Bunun iki nedeni çoğu blok şifredeki anahtar planlama algoritmalarında bulunan yavaş yayılım ve bit sızıntısı zaaflarıdır (bit leakage) [48]. Örneğin AES blok şifresinde kullanılan anahtar planlama algoritmasında bu zaaflar mevcuttur ve bu zaaflar çeşitli saldırılarda saldırının başarımını kolaylaştıran yardımcı öğe olarak kullanılmaktadır [48] [49]. Tasarımı yapılan bir anahtar planlama algoritması için katı çığ testi (belli bir güven aralığı çerçevesinde) yavaş yayılımın test edilmesinde kullanılabilir. Bit sızıntısı zaafı ise yapılan tasarımla ilgilidir ve herhangi bir alt anahtarın bir saldırı

sonucu elde edilmesi durumunda diğer alt anahtarların veya gizli anahtarın (veya bunların bir parçasının) elde edilebilmesini tanımlar. Bit sızıntısı zaafının önüne geçmek için alt anahtarların birbirinden bağımsız olarak üretilmesi bir çözüm yöntemi olarak kullanılabilir.

3.4. Kriptoanaliz

Kriptoanaliz kısaca şifre kırma bilimidir ve kriptografik yapıların kırılmasında kullanılan tekniklerin çalışılması anlamına gelmektedir [50]. Diğer yandan kriptoanaliz bilimi bir şifrenin gücünün değerlendirilmesinde de kullanılır. Daha güçlü şifrelerin geliştirilmesi yeni tür saldırıların (kriptoanaliz tekniklerinin) geliştirilmesi ile mümkün hale gelir.

Bir kriptosistemin güvenliği söz konusu olduğunda önemli yaklaşımlar aşağıdaki gibi ifade edilebilir [51][52]:

- Hesaplanabilir güvenlik (Conditional security),
- İspatlanabilir güvenlik (Provable security),
- Şartsız güvenlik (Unconditional security).

Hesaplanabilir güvenlik yaklaşımı bir kriptosistemi kırabilmek için gerekli hesaplama çabasını ifade eder. Herhangi bir kriptosistemin kırılabilmesi için N işlem (N çok büyük bir değer olmak üzere) gerekiyorsa hesaplanabilir güvenli bir kriptosistem tanımlanabilir. Bu tanım altında güvenliği ispatlanmış kriptosistemler uygulamada bulunmamaktadır. Pratikte bir kriptosistemin hesaplanabilir güvenliğinin tayininde genellikle bazı özel saldırı tipleri (örneğin geniş anahtar arama (brute force) saldırısı) kullanılır. Bu güvenlik yaklaşımına uygun şifrelere örnek olarak blok şifreler verilebilir.

İspatlanabilir güvenlik yaklaşımı bir kriptosistemin güvenliğini bazı önemli zor problemlere indirgeyerek güvenlik ispatı sağlar. Bu yaklaşım belli bir tip probleme karşı güvenlik ispatı sağladığı için kesin güvenlik ispatı sağlamaz. Bu güvenlik yaklaşımına örnek olarak RSA asimetrik şifreleme algoritması verilebilir. Bu şifreleme algoritmasının gücü, büyük sayıların çarpanlara ayırabilme probleminin zorluğuna dayanır.

Şartsız güvenlik yaklaşımı bir kriptosistem sonsuz hesaplama kaynağına sahip olunduğu halde kırılamıyorsa o kriptosistem için şartsız güvenli tanımı yapılır. Bu güvenlik yaklaşımına örnek olarak tek kullanımlık şerit (one time pad) şifresi verilebilir. Bu şifrelerde anahtar tamamen rassal olmalı ve bir kereliğine kullanılmalıdır.

Bir kriptosisteme karşı geliştirilen saldırıların amacı herhangi bir şifreli metin için şifre çözme yeteneğinin kazanılabilmesidir. Bu yeteneğin kazanılması da anahtarı elde etme (total break), geliştirilen bir algoritma yoluyla anahtarı bilmeden şifreli metinlerin çözülmesi (global deduction) veya anahtar, açık metin ve şifreli metin hakkında bilgi sahibi olmak (information deduction) şeklinde olabilir.

Herhangi bir kriptosisteme olan saldırıda saldırganın kriptosistemi bildiği kabul edilir. Bu prensibe Kerchhoff'un prensibi adı verilir [53]. Buna ek olarak saldırganın kriptosistem hakkında sahip olduğu bazı bilgiler olabilir (gizli anahtar hariç). Bu sahip olduğu bilgilere göre saldırı modellerinden birini seçebilir. En yaygın saldırı modelleri aşağıdaki gibi verilebilir [51][53]:

- Sadece şifreli metin saldırısı (Ciphertext-only attack): Saldırgan şifreli metine/metinlere sahiptir.
- Bilinen açık metin saldırısı (Known-plaintext attack): Saldırgan açık metinlere ve bu açık metinlere karşılık şifreli metinlere sahiptir. Kısaca açık metin/şifreli metin çiftlerine sahiptir.
- Seçilmiş açık metin saldırısı (Chosen-plaintext attack): Saldırgan açık metinleri seçebilir ve bu açık metinlerin şifreli metinlerini elde edebilir.
- Seçilmiş şifreli metin saldırısı (Chosen-ciphertext attack): Saldırgan şifreli metinleri seçebilir ve bu şifreli metinlerin açık metinlerini elde edebilir.

Geliştirilen kriptoanaliz yöntemleri (veya saldırı yöntemleri) verilen saldırı modellerinden birini kullanır. Örneğin doğrusal kriptoanaliz bilinen açık metin saldırı modeline, differensiyal kriptoanaliz seçilmiş açık metin saldırı modeline uygun kriptoanaliz yöntemleridir. Bu saldırı modelleri dışında uyarlamalı seçilmiş açık metin

(adaptive chosen-plaintext), uyarlamalı olmayan seçilmiş şifreli metin (non-adaptive chosen-plaintext) ve ilişkili anahtar saldırı (related-key attack) modellleri gibi saldırı modelleri bulunmaktadır. Yukarıda verilen saldırı modelleri pratikte uygulanabilirliği kolaydan daha zora doğru sıralanmıştır ve içlerindeki en gerçekçi saldırı modeli sadece şifreli metin saldırısıdır. Gerçekçi olmayan bir saldırı modeli kullanılarak geliştirilen kriptoanaliz yöntemlerine karşı dayanıklılık şifrelerin güvenliğine bir güvenlik payı koymaktadır.

Bir şifreye yapılan saldırılar değerlendirilirken üç faklı karmaşıklık ölçütü bulunmaktadır [54]:

- Veri karmaşıklığı (Data complexity),
- Zaman karmaşıklığı (Time complexity),
- Bellek karmaşıklığı (Memory complexity).

Veri karmaşıklığı, saldırı için gerekli veri miktarıdır (saldırı modeline göre şifreli metinlerin sayısı veya açık metin/şifreli metin çiftlerinin sayısı). Zaman karmaşıklığı saldırıda gerekli adımların (örneğinin şifreleme işlemlerinin) sayısıdır. Buna ek olarak zaman karmaşıklığı ön hesaplama karmaşıklığı (pre-computational complexity) ve sonraki hesaplama karmaşıklığı (post-computational complexity) olarak ikiye ayrılabilir. Ön hesaplama kısmı genellikle bir kere yapılan ve anahtar bitleri gözlenmeden olan işlemleri kapsar. Sonraki zaman karmaşıklığında ise tüm anahtar bitleri gözlenirken meydana gelen işlemler göz önüne alınır. Bellek karmaşıklığı saldırıda kullanılan bellek miktarı ile ilgilidir. Tüm karmaşıklık parametreleri, her tür saldırı için uygun olmayabilir. Dolayısıyla saldırıların paremetre tabanlı olarak karşılaştırılması daha uygundur. Örneğin, bir saldırı türü için zaman karmaşıklığı önemli iken kullanılan bellek miktarı saldırı ile ilgili olmayabilir.

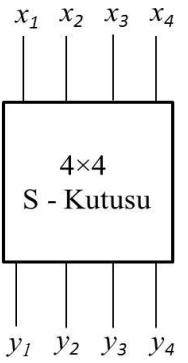
3.4.1. Doğrusal Kriptoanaliz

Doğrusal Kriptoanaliz [8] Matsui tarafından 1993 yılında yılında teorik bir saldırı olarak geliştirilmiş ve daha sonra DES blok şifresine karşı başarıyla uygulanmış bir istatistiksel saldırı türüdür. Verilen saldırı modellerinden bilinen açık metin saldırısı modeline uygun

bir saldırıdır. Bu saldırının temelinde açık metin ve şifreli metin bitleri arasında kurulan yüksek olasılıklı doğrusal ifadelerin elde edilmesi bulunmaktadır. Bir şifreye saldırı sırasında doğrusal olmayan S-kutularından yüksek olasılıklı doğrusal ifadeler elde edilir ve bu doğrusal ifadeler birleştirilerek bilinmeyen anahtar bitleri elde edilmeye çalışılır. Doğrusal kriptoanalizin uygulanabilmesi için $n \times m$ boyutunda bir S-kutusunun giriş ve çıkış bitleri arasında sapma (bias) değerleri (ε) yüksek ($\frac{1}{2}$ den + ya da - yönde) doğrusal ifadeler aşağıda verilen formdaki gibi elde edilir:

$$x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_n} \oplus y_{i_1} \oplus y_{i_2} \oplus \ldots \oplus y_{i_m} = 0$$

Yukarıda verilen ifadede x_i, y_i değerleri sırasıyla S-kutusunun giriş ve çıkış bitlerini temsil etmektedir. Doğrusal kriptoanalizin uygulanması sırasında tüm olası $(2^n - 1) \cdot (2^m - 1)$ doğrusal ifade incelenerek yüksek olasılıklı olanlar saldırıda değerlendirilir. Bir S-kutusu için doğrusal yaklaşımların olasılıkları S-kutusu için elde edilen LAT tablosu ile doğrudan ilişkilidir.



Şekil 3.3. 4×4 Boyutunda Bir S-kutusunun Genel Gösterimi

Örnek 3.13. PRESENT S-kutusu için $x_2 \oplus x_4 \oplus y_1 \oplus y_3 = 0$ ifadesinin sapma değeri ε'u elde edelim.

Şekil 3.3'e göre PRESENT S-kutusunu değerlendirirsek verilen ifadeye karşılık LAT tablosu giriş ve çıkış maskesi sırasıyla $\Gamma_A = 5$ ve

$\Gamma_B = \mathrm{A}$ olacak şekilde hexadecimal değerlere karşılık gelir. PRESENT S-kutusu için $LAT(5,A) = -4$ olduğundan verilen denklemin sağlanma olasılığı $p = \frac{8-4}{16} = \frac{1}{4}$'tür. Dolayısıyla denklemin sapma değeri $\varepsilon = p - \frac{1}{2}$ olacağından $\varepsilon = \frac{1}{4} - \frac{1}{2} = -\frac{1}{4}$ olarak elde edilir.

Doğrusal kriptoanaliz sırasında açık metin bitleri ve şifreli metin bitleri arasında elde edilen yüksek olasılıklı doğrusal ifadede yer alan S-kutularına aktif S-kutusu adı verilir. Doğrusal kriptoanaliz, bu yüksek olasılıklı doğrusal ifade, açık metin bitleri ve son döngüde kullanılan S-kutularına giriş olan durum bitleri kullanılarak gerçekleştirilir. Bu yüksek olasılıklı doğrusal ifadede birçok S-kutusu (aktif S-kutuları) ve bu S-kutularının doğrusal yaklaşımlarının bir toplamı yer almaktadır. P toplam doğrusal yaklaşımın olasılığı aşağıdaki gibi elde edilebilir:

$$P = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} (p_i - \frac{1}{2})$$

Verilen ifadede n aktif S-kutularının sayısını ve p_i aktif S-kutuları için elde edilen doğrusal ifadelerin olasılıklarını temsil eder. Saldırının devamında şifrenin son döngüdeki durum bitleri, bilinen açık metinlere ait şifreli metinler aracılığı ile tüm olası kısmi anahtar bitleri için kısmi şifre çözme işlemi ile elde edilir. Kısmi şifre çözme işlemlerinde kullanılan anahtarlar arasından doğrusal ifadenin mutlak sapmasına yakın (veya mutlak sapması en yüksek değer) anahtar doğru anahtar olarak tayin edilir. Yanlış anahtarlara ait sapmalar ise 0 veya 0 değerine yakın değerler olarak beklenir. Saldırının uygulanmasında kullanılan açık metin/şifreli metin çiftlerinin sayısı $\frac{c}{\varepsilon_T{}^2}$ şeklinde verilebilir. Burada ε_T açık metin bitleri ile S-kutusuna giriş olan durum bitleri arasındaki doğrusal ifade için toplam sapma miktarı ve c uygulamanın başarımı için kullanılan (6, 8 veya 10 olabilir) sabittir.

Aktif S-kutularının sayısı ne kadar fazla ise doğrusal ifadede elde edilebilecek yüksek olasılıklı sapma azalır. Dolayısıyla şifreye karşı

doğrusal kriptoanaliz zorlaşır. Bir şifrenin doğrusal kriptoanalize karşı dayanıklılığı söz konusu olduğunda minimum aktif S-kutusu sayısı ve S-kutusunun LAT tablosundaki en büyük mutlak değer göz önüne alınmalıdır. Bu değere göre doğrusal kriptoanaliz saldırısının etkisiz hale geleceği bir sınır döngü sayısı elde edilebilir. Doğrusal kriptoanaliz ve basit bir blok şifreye uygulaması hakkında daha detaylı bilgi [55]'den elde edilebilir.

S-kutuları için tanımlanan doğrusal olasılık (linear probability) [56], bir şifrede doğrusal kriptoanaliz saldırısında kullanılacak minimum aktif S-kutusu sayısı bilindiğinde şifrenin doğrusal kriptoanalize karşı dayanıklılığını kabaca elde etmemizi sağlayan önemli bir parametredir ve $m \times m$ bir S-kutusu için aşağıdaki tanımlanabilir:

$$LP_S(\Gamma_A, \Gamma_B) = \left(\frac{\{x \in F_2^m | \Gamma_A \bullet x = \Gamma_B \bullet S(x)\}}{2^{m-1}} - 1 \right)^2$$

S-kutusunun LAT değerindeki en kötü durum (en büyük mutlak değer) için elde edilebilecek maksimum doğrusal olasılık değeri ise (özellikle) bir SPN tabanlı şifre tasarımında gerekli minimum döngü sayısı (doğrusal kriptoanalize karşı) belirlememize yardımcı olur. Örneğin PRESENT S-kutusu için en büyük doğrusal olasılık bu S-kutusu için maksimum mutlak LAT değeri 4 olduğu için $LP_{P-\max} = \left(\frac{8+4}{8} - 1 \right)^2 = \frac{1}{4}$ olarak elde edilebilir.

Örnek 3.14. 128-bit anahtar ve 128-bit AES blok şifresi için doğrusal kriptoanalizin etkisiz hale geldiği sınır döngü sayısını elde edelim.

AES blok şifresi için 4 döngüde ShiftRows ve MixColumns dönüşümlerinin etkileri ile beraber minimum aktif S-kutusu sayısının 25 olduğu Bölüm 3.2'de belirtilmişti. AES S-kutusunun sahip olduğu maksimum doğrusal olasılık değeri bu S-kutusunun en büyük mutlak LAT değeri 16 olduğu için $LP_{AES-\max} = \left(\frac{128+16}{128} - 1 \right)^2 = \frac{1}{64} = 2^{-6}$ olarak elde edilebilir. Dolayısıyla AES blok şifresi için maksimum doğrusal olasılık 4 döngü sonunda $(2^{-6})^{25} = 2^{-150}$ şeklindedir ve 128-bit gizli anahtara sahip

4 döngülük AES şifresi için maksimum doğrusal olasılık $2^{-150} \leq 2^{-128}$ ile sınırlıdır. Sonuç olarak AES blok şifresinin doğrusal kriptoanalize karşı dayanıklı olabilmesi için gerekli minimum döngü sayısı 4'tür.

3.4.2. Diferansiyel Kriptoanaliz

Diferansiyel kriptoanaliz [9] Biham tarafından 1991 yılında geliştirilmiş bir istatistiksel saldırı türüdür. Verilen saldırı modellerinden seçilmiş açık metin saldırısı modeline uygun bir saldırıdır. Bu saldırının temelinde açık metin çiftlerindeki özel farkların sonuçlanan şifreli metinlerde oluşturduğu farkın etkisini analiz etme bulunmaktadır. Saldırının gerçekleştirilmesi için şifrede kullanılan doğrusal olmayan yapı/yapılar (örneğin S-kutuları) için diferansiyel farklar incelenerek yüksek diferansiyel farklar tüm şifre için kullanışlı bir diferansiyel karakteristik elde etmede kullanılır. Saldırı için elde edilen diferansiyel karakteristik, S-kutularında meydana gelen farkları birleştirir ve bu karakteristik sadece şifreli metin ve açık metin bitlerini ilgilendirir.

Diferansiyel kriptoanaliz saldırısında saldırganın elinde çok sayıda açık metin/şifreli metin çiftlerine (x_1, x_2, y_1, y_2) sahip olduğu kabul edilir ve saldırgan açık metinleri $\Delta x = x_1 \oplus x_2$ olacak şekilde seçebilir. Saldırgan, bu Δx farkına karşılık algoritmadan yüksek olasılıkta meydana gelen Δu (şifrenin son döngüde ki S-kutusundan önceki durum bitleri) farkını bulur ve her açık/şifreli metin çiftleri için olası kısmi anahtar değerlerini dener. Bu denemelerde Δu farkı tutması halinde sayaç değerini o anahtar değeri için 1 arttırır. Yüksek olasılığı yakalayan anahtar değeri şifrede kullanılan doğru anahtar değeri olarak tayin edilir. Saldırının uygulanmasında kullanılan seçilmiş açık metin/şifreli metin çiftlerinin sayısı $\frac{c}{p}$ şeklinde verilebilir. Burada p saldırıda kullanılan diferansiyel karakteristiğin olasılığı ve c uygulamanın başarımı için kullanılan (6, 8 veya 10 olabilir) sabittir.

Doğrusal kriptoanalizdekine benzer şekilde diferansiyel kriptoanalizde de elde edilen karakteristik içerisinde yer alan S-kutularına aktif S-kutusu adı verilir. Diferansiyel karakteristik içerisinde bulunan aktif S-kutularının sayısı ne kadar yüksek ise diferansiyel karakteristiğin olasılığı düşer ve dolayısıyla şifreye karşı gerçekleştirilecek diferansiyel kriptoanaliz zorlaşır. Bir şifrenin diferansiyel kriptoanalize karşı dayanıklılığı söz konusu olduğunda diferansiyel karakteristikte bulunabilecek minimum aktif S-kutusu sayısı ve kullanılan S-kutusunun Fark Dağılım Tablosundaki en büyük değer önem kazanır. Bu değerlere göre diferansiyel kriptoanaliz saldırısının etkisiz hale geleceği bir sınır döngü sayısı elde edilebilir. Diferansiyel kriptoanaliz ve basit bir blok şifreye uygulaması hakkında daha detaylı bilgi [55]'den elde edilebilir.

S-kutuları için tanımlanan diferansiyel olasılık (differential probability) [56], bir şifrede diferansiyel kriptoanaliz saldırısında kullanılacak minimum aktif S-kutusu sayısı bilindiğinde şifrenin diferansiyel kriptoanalize karşı dayanıklılığını kabaca elde etmemizi sağlayan önemli bir parametredir ve $m \times m$ bir S-kutusu için aşağıdaki tanımlanabilir:

$$DP_S(a,b) = \frac{\#\left\{x \in F_2^m \mid S(x) + S(x+a) = b\right\}}{2^m}$$

S-kutusunun Fark Dağılım Tablosundaki en kötü durum (bu tablodaki en büyük değer) için elde edilebilecek maksimum diferansiyel olasılık değeri ise (özellikle) bir SPN tabanlı şifre tasarımında gerekli minimum döngü sayısı (diferansiyel kriptoanalize karşı) belirlememize yardımcı olur. Örneğin PRESENT S-kutusu için en büyük diferansiyel olasılık bu S-kutusu için maksimum Fark Dağılım Tablosu değeri 4 olduğu için $DP_{P-\max} = \frac{4}{16} = \frac{1}{4}$ olarak elde edilebilir.

Örnek 3.15. 128-bit anahtar ve 128-bit AES blok şifresi için diferansiyel kriptoanalizin etkisiz hale geldiği sınır döngü sayısını elde edelim.

AES blok şifresi için 4 döngüde ShiftRows ve MixColumns dönüşümlerinin etkileri ile beraber diferansiyel karakteristikte bulunabilecek minimum aktif S-kutusu sayısının 25 olduğu Bölüm 3.2'de belirtilmişti. AES S-kutusu için maksimum diferansiyel olasılık bu S-kutusunun en büyük Fark Dağılım Tablosu değeri 4 olduğundan $DP_{AES-\max} = \frac{4}{256} = 2^{-6}$ olarak elde edilebilir. Dolayısıyla AES blok şifresi için maksimum diferansiyel olasılık 4 döngü sonunda $(2^{-6})^{25} = 2^{-150}$ şeklindedir ve 128-bit gizli anahtara sahip 4 döngülük AES şifresi için maksimum diferansiyel olasılık $2^{-150} \leq 2^{-128}$ ile sınırlıdır. Sonuç olarak AES blok şifresinin diferansiyel kriptoanalize karşı dayanıklı olabilmesi için gerekli minimum döngü sayısı 4'tür.

3.5. Değerlendirmeler

Bu bölümde kriptografik test yöntemleri ve kriptoanaliz konusunda bir incelemeye yer verilmiştir. Şifre tasarımında kullanılan önemli bileşenlerin tasarımı da bu konu ile ilgili olarak irdelenmelidir. Bir şifreleme algoritmasının olabildiğince rassal çıktılar üretmesinin gerekliliği yanında önemli saldırı tekniklerine karşı dayanıklı olması istenen özellikler arasındadır. Literatürde blok şifrelerin tasarımları ile ilgili olarak belli bir birikime sahip olunmuştur. Ancak özellikle akış şifreleri için aynı durum söz konusu değildir. Son zamanlarda daha az güç tüketimi sağlayan hafif sıklet blok şifrelerin geliştirilmesi popüler olmuştur. Bölümde bahsedilen test yöntemleri ve kriptoanaliz teknikleri bu şifreler için de uygulanabilir. Bununla beraber hafif sıklet yapılarda kullanılan yayılım tabakalarında bit permütasyonlarının tercihi ile donanım uygulamalarında daha hızlı ve daha az maliyetli şifreler geliştirilebilirken S-kutularının çıkış bitlerini doğrudan kullanan bu yapılar S-kutuları için yeni kriptografik ölçütleri de beraberinde getirmektedir. Ayrıca bölüm içerisinde bahsedilen doğrusal ve diferansiyel kriptoanaliz tekniklerinin yanı sıra kesik diferansiyel kriptoanaliz (truncated differential cryptanalysis) [57], imkânsız diferansiyel kriptoanaliz (impossible differential cryptanalysis) [58] [59] ve çoklu set saldırıları (multiset at-

tack) [60] gibi önemli farklı saldırı tekniklerinin de bir şifrenin dayanıklılığının değerlendirilmesinde kullanıldığını unutmamak gerekir.

Teşekkür

Bu önemli bölümün hazırlanmasında yardımlarını esirgemeyen değerli arkadaşım Doç. Dr. Sedat Akleylek'e ve sevgili eşim Dr. Öğr. Üyesi Fatma Büyüksaraçoğlu Sakallı'ya teşekkür ederim.

Kaynaklar

[1] B.A. Forouzan, Cryptography and Network Security, International Edition, McGraw-Hill Education, 2008.

[2] FIPS 46-3, Data Encryption Standard, Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., October 25, 1999.

[3] FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., November 26, 2001.

[4] B. Schneier, Applied Cryptography - Protocols, Algorithms, and Source code in C, John Wiley & Sons, Inc., 2nd edition, 1996.

[5] C. De Cannière and B. Preneel, The Stream Cipher Trivium, eSTREAM, the ECRYPT Stream Project., 2005, available at: http://www.ecrypt.eu.org/stream.

[6] H. Wu, A New Stream Cipher HC-256, FSE 2004, LNCS, Vol. 3017, pp. 226-244, Springer, 2004.

[7] E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet, and W. Jalby. Collisions of SHA-0 and Reduced SHA-1, EUROCRYPT 2005, LNCS, Vol. 3494, pp. 36–57. Springer, 2005.

[8] M. Matsui, Linear cryptanalysis method for DES cipher, EUROCRYPT'93, LNCS, Vol.765, pp. 386-397, 1994.

[9] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, CRYPTO'90, LNCS, Vol. 537, pp. 2-21, 1990.

[10] L.E. Bassham III, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. Sp 800-22 rev. 1a., A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Gaithersburg, MD, United States, 2010.

[11] A. Canteaut, Stream Ciphers, Encyclopedia of Cryptography and Security, 2005, available at: http://www-rocq.inria.fr/codes/Anne.Canteaut/encyclopedia.pdf

[12] A. Braeken, Cryptographic Properties of Boolean Functions and S-Boxes, Ph.D. Thesis, K.U. Leuven, Leuven, Belgium, March 2006.

[13] A. Canteaut and E. Filiol, On the Influence of the Filtering Function on the Performance of Fast Correlation Attacks on Filter Generators, In Symposium on information theory in the Benelux, May 2002.

[14] N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, EUROCRYPT 2003, LNCS, Vol. 2656, pp. 345-359, 2003.

[15] J. Fuller, Analysis of Affine Equivalent Boolean Functions for Cryptography, Ph.D. Thesis, Queensland University of Technology, Brisbane, Queensland, Australia, December 2003.

[16] L. Keliher, Linear Cryptanalysis of Substitution-Permutation Networks, Ph.D. Thesis, Queen's University, Kingston, Ontario, Canada, October 2003.

[17] J. Dillon, A Survey of Bent Functions, Tech. Report, NSA Technical Journal, pp. 191-215, unclassified, 1972.

[18] W. Meier, E. Pasalic, and C.Carlet, Algebraic Attacks and Decomposition of Boolean Functions, Eurocrypt 2004, LNCS, Vol. 3027, Springer-Verlag, pp. 474-491, 2004.

[19] T. Siegenthaler, Correlation–immunity of Nonlinear Combining Functions for Cryptographic Applications, IEEE Transactions on Information Theory, Vol. IT-30, No. 5, pp. 776-780, 1984.

[20] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J., Vol. 28, pp. 656–715, 1949.

[21] K. Nyberg, Differentially Uniform Mappings for Cryptography, EUROCRYPT'93, LNCS, Vol. 765, pp. 55-64, 1994.

[22] I. Vergili, Statistics on Satisfaction of Security Criteria for Randomly Generated S-boxes, M.S. Thesis, Middle East Technical University, Ankara, Türkiye, 2000.

[23] S. Kavut and M.D. Yücel, On Some Cryptographic Properties of Rijndael, Lecture Notes in Computer Science: Information Assurance in Computer Networks, Methods, Models and Architectures for Network Security, LNCS, Vol.2052, Springer-Verlag, pp.300-311, 2001.

[24] J.B. Kam and G.I. Davida, Structured Design of Substitution Permutation Encryption Networks, IEEE Transactions on Computers, Vol. C-28, No.10, pp. 747-753, 1979.

[25] H. Feistel, Cryptography and Computer Privacy, Scientific American, Vol. 228, No. 5, pp.15-23, 1973.

[26] F. Webster and S.H. Tavares, On the Design of S-boxes, Advances in Cryptology, CRYPTO'85, Vol. 218, Springer Verlag, pp. 523-534, 1986.

[27] M. Matsui, The First Experimental Cryptanalysis of the Data Encryption Standard, Advances in Cryptology, CRYPTO'94, LNCS, Vol. 839, Springer-Verlag, pp. 1-11, 1994.

[28] S. Çeçen, Nonlinearity and Propagation Characteristics of Substitution Boxes, M.S. Thesis, Middle East Technical University, Ankara, Türkiye, 2001.

[29] H. Heys, A Tutorial on Linear and Differential Cryptanalysis, Cryptologia, Vol 26, No. 3, pp. 189-221, 2002.

[30] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, Vol. 4, No. 1, pp. 3-72, 1991.

[31] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar C, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher, Cryptographic Hardware and Embedded Systems - CHES 2007, LNCS, Vol. 4727, Springer, Berlin, Heidelberg, 450-466, 2007.

[32] S. Mister and C.M. Adams, Practical S-Box Design, SAC'96- Third Annual Workshop on Selected Areas in Cryptography, Queen's Univ., Kingston, Ontario, Canada, pp. 61-76, August 1996.

[33] M.R. Z'aba, Analysis of linear relationships in block ciphers, Ph.D. Thesis, Queensland University of Technology, Brisbane, Australia, 2010.

[34] B. Aslan, M.T. Sakallı, Algebraic construction of cryptographically good binary linear transformations, Security and Communication Networks, Vol. 7, No. 1, pp. 53-63, 2014.

[35] D. Kwon, J. Kim, S. Park, S.H. Sung, Y. Sohn, J.H. Song, Y. Yeom, E-J. Yoon, S. Lee, J. Lee, S. Chee, D. Han, J. Hong, New block cipher: ARIA. In Proceedings of International Conference on Information Security and Cryptology, LNCS, vol. 2971, Springer-Verlag, pp. 432-445, 2004.

[36] F.J. MacWilliams, N.J.A. Sloane, The theory of error-correcting codes, North Holland Publishing Co., North-Holland, Amsterdam, 1977.

[37] W. Bosma, J. Cannon, C. Playoust, The Magma Algebra System I: the user language. Journal of Symbolic Computation, Vol. 24, No. 3-4, pp. 235–265, 1997.

[38] Magma Calculator, available at: http://magma.maths.usyd.edu.au/calc/.

[39] A.M. Youssef, S. Mister, S.E. Tavares, On the design of linear transformation for substitution-permutation encryption networks, In Proceedings of Selected Areas in Cryptography (SAC'97), pp. 40-48, 1997.

[40] M. Sajadieh, M. Dakhilalian, H. Mala, B. Omoomi, On construction of involutory MDS matrices from Vandermonde matrices in GF(2q), Designs, Codes and Cryptography, Vol 64, No. 3, pp. 287-308, 2012.

[41] M.K. Pehlivanoğlu, M.T. Sakallı, S. Akleylek, N. Duru, V. Rijmen, Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography, IET Information Security, Vol. 12, No. 4, pp. 348-355, 2018.

[42] S. Akleylek, M.T. Sakallı, E. Öztürk, A.Ş. Mesut, G.Tuncay, Generating binary diffusion diffusion layers with maximum/high branch numbers and low search complexity, Security and Communication Networks, Vol 9, No 16, pp. 3558-3569, 2016.

[43] M.T. Sakallı, S. Akleylek, B. Aslan, E. Buluş, F.B. Sakallı, On the Construction of 20×20 and 24×24 Binary Matrices with Good Implementation Properties for Lightweight Block Ciphers and Hash Functions, Mathematical Problems in Engineering, Vol. 2014, Article ID 540253, 12 pages, 2014.

[44] S. Akleylek, V. Rijmen, M.T. Sakallı, E. Öztürk, Efficient methods to generate cryptographically significiant binary diffusion layers, IET Information Security, Vol. 11, No. 4, pp. 177-187, 2017.

[45] M.T. Sakallı, B. Aslan, On the algebraic construction of cryptographically good 32×32 binary linear transformations, Journal of Computational and Applied Mathematics, Vol. 259, Part B, pp. 485-494, 2013.

[46] K. Khoo, T. Peyrin, A.Y. Poschmann, H. Yap, FOAM: searching for hardware-optimal SPN structures and components with a fair comparison'. In Proceedings of Cryptographic Hardware and Embedded Systems (CHES 2014), LNCS, Vol. 8731, Springer, pp. 433–450, 2014.

[47] E. Biham, New types of cryptanalytic attacks using related keys, Advances in Cryptology-EUROCRYPT'93, LNCS, Vol. 765, pp. 398-409, Springer-Verlag, 1994.

[48] L. May, M. Henricksen, W. Millan, G. Carter, and E. Dawson, Strengthening the Key Schedule of the AES, In Proceedings of the 7th Australasian Conference on Information Seucurity and Privacy (ACISP 2002), LNCS, Vol. 2384, Springer, pp. 226-240, 2002.

[49] R.C.W. Phan, Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES), Information Processing Letters Vol. 91, No. 1, pp. 33-38, 2004.

[50] M.T. Sakallı, Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi, Ph.D. Thesis, Trakya Universitesi, Edirne, 2006.

[51] D.R. Stinson, Cryptography: Theory and Practice, Second Edition, CRC Press, 2002.

[52] B. Preneel, Analysis and Design of Cryptographic hash functions, Ph.D. Thesis, Katholieke Universiteit Leuven, January 1993.

[53] V. Rijmen, Cryptanalysis and Design of Iterated Block Ciphers, PHd Thesis, Katholieke Universiteit Leuven, October 1997.

[54] J. Nakahara, Cryptanalysis and Design of Block Ciphers, Ph.D. Thesis, Katholieke Universiteit Leuven, June 2003.

[55] H. Heys, A Tutorial on Linear and Differential Cryptanalysis, Cryptologia, Vol. 26, No. 3, pp. 189-221, 2002.

[56] K. Chun, S. Kim, S. Lee, S.H. Sung, S. Yoon, Differential and linear cryptanalysis for 2-round SPNs, Information Processing Letters, Vol. 87, No. 5, pp. 277-282, 2003.

[57] L.R. Knudsen, Truncated and Higher Order Differentials, FSE'94, Vol. 1008, Springer-Verlag, pp. 196-211, 1995.

[58] E. Biham, A. Biryukov, and A. Shamir, Cryptanalysis of Skipjack reduced to 31 rounds using Impossible Differentials, Advances in Cryptology - EUROCRYPT'99, LNCS, Vol. 1592, Springer-Verlag, pp. 55-64, 1996.

[59] R.C.W. Phan, Impossible Differential Cryptanalysis of Mini-AES, Cryptologia, Vol. 27, No. 4, 2003.

[60] J. Daemen, L.R. Knudsen, and V. Rijmen, The block cipher square, FSE'97, LNCS, Vol. 1267, Springer Verlag, pp. 149-165, 1997.

Kuantum Bilgisayarlar ile Kriptoanaliz ve Kuantum Sonrası Güvenilir Kripto Sistemleri

BÖLÜM 4

Sedat AKLEYLEK - Meryem SOYSALDI

KUANTUM BİLGİSAYARLAR İLE KRİPTOANALİZ VE KUANTUM SONRASI GÜVENİLİR KRİPTO SİSTEMLERİ

Bilginin saklanması ve güvenli bir şekilde iletilmesi için çeşitli kriptosistemler geliştirilmiştir. Hesaplama gücü arttıkça sistemlerin güvenli olmadıkları ispatlanmış ve kırılan sistemlerin yerine daha güvenli olan sistemler oluşturulmuştur. Günümüzde kullanılan asimetrik/açık anahtarlı kriptosistemler var olan hesaplama gücüyle hesaplanması zor olan problemlere dayanmaktadır. Google ve IBM gibi büyük şirketler kuantum bilgisayarlara sahip olduklarını açıklamışlardır. Bunun yanı sıra, RSA, DSA ve ECDSA gibi çarpanlarına ayırma veya ayrık logaritma problemlerine dayanan günümüz kriptosistemleri kuantum algoritmalar ile kuantum bilgisayarlarda polinom zamanda çözülerek güvensiz hale gelmektedir. Bilgi ve iletişim çağında cihazların birbirini güvenli bir şekilde tanıyabilmesi, güvenilir veri paylaşımının sağlanması gibi konular için farklı çözüm önerileri bulunmaktadır. Bu çözüm önerileri hesaplama gücündeki ve/veya hedef cihazdaki sistem kaynaklarındaki gelişmelere bağlı olarak sürekli değişimler göstermektedir. Bu değişimler neticesinde; kuantum bilgisayarlarda çalışan algoritmalara karşı bile güvenilir; gizlilik, bütünlük, kimlik denetimi ve inkar edememe kavramlarını sağlayacak kriptosistemlere ihtiyaç bulunmaktadır. Bu çalışmada, kuantum algoritmalardan olan Shor ve Grover tarafından önerilen algoritmalara yer verilmiştir. Kuantum sonrası kriptosistemlerin oluşturulması için güvenilir olduğu bilinen kriptosistem sınıfları ele alınmıştır.

4.1. Giriş

Kriptografi gizlilik, bütünlük, kimlik doğrulama ve inkâr edememe gibi kavramlar ile bilginin güvenliğini sağlamak amacıyla oluşturulmuş matematiksel tekniklerin bütünüdür [1]. İhtiyaca bağlı olarak bilgi güvenliği kavramlarını sağlayabilmek adına farklı özellikte kriptosistemler ortaya çıkmıştır. Bu sistemler üç grup olarak nitelendirilmektedir: Gizli anahtarlı, açık anahtarlı ve anahtarsız kriptosistemler.

Simetrik kriptosistemler olarak da adlandırılan gizli anahtarlı sistemlerde alıcı ve gönderici ortak bir anahtar üzerinde anlaşmaktadır. Dolayısıyla şifreleme ve şifre çözme işlemlerinde tek bir gizli anahtar kullanılmaktadır [1]. Alıcı ve göndericinin ortak bir gizli anahtar üzerinde anlaşmak zorunda olması gizli anahtarın güvenli bir şekilde dağıtılması problemini beraberinde getirmiştir. Diffie-Hellman tarafından bu probleme çözüm olarak önerilen anahtar değişim algoritması ile açık anahtarlı kriptosistemler ortaya çıkmıştır.

Simetrik ve asimetrik kriptosistemlerin yanı sıra anahtarsız kriptosistemler de bulunmaktadır. Kriptografik özet/kıyım fonksiyonları, anahtar kullanmayan kriptosistemlerdendir. Kriptografik özet fonksiyonları, herhangi bir uzunluktaki açık metni alarak sabit uzunlukta bir çıktı (özet) üretmektedir. Güvenilir bir özet fonksiyonu için sabit uzunlukta üretilen özet değerine karşılık gelen açık metni elde etmek ve aynı özet değerine karşılık gelen iki farklı metni bulmak zor olmalıdır.

Günümüz bilgisayarların hesaplama gücü transistör sayısı ile doğru orantılı bir şekilde artmaktadır. Moore yasasına göre bilgisayarlarda bulunan transistörler her iki yılda bir neredeyse iki katına çıkmaktadır [2]. Oda büyüklüğündeki ilk bilgisayarlardan günümüz bilgisayarlara kadar transistör sayısındaki artış göz önüne alındığında ilerlemenin üst düzeylerde olduğu görülmektedir. Bilgisayarların hesaplama gücünün daha da arttırılabilmesi için klasik bilgisayar yapısının değiştirilmesi gerekmektedir. 1982 yılında Richard Feymann klasik fizik kanunları yerine kuantum mekaniğini temel alan kuantum

bilgisayarların oluşturulabileceği fikrini ortaya atmıştır [3]. Bu fikir ile beraber kuantum bilgisayar oluşturma çalışmaları başlamıştır. 1997 yılında iki kübitlik ilk kuantum bilgisayar oluşturulmuştur [4]. Tablo 4.1 'de bazı büyük şirketlerin ürettiği kuantum bilgisayarlar, kübit sayıları, kuantum bilgisayarları oluştururken kullandıkları teknoloji ve model verilmektedir [5]. Tablo 4.1 'de bir kısmı verilen kuantum bilgisayarlar her amaca uygun şekilde tasarlanmamıştır. Örneğin; IBM'in kuantum bilgisayar ve simülatörünü geliştirme amacı; ticari olarak üçüncü taraflarla işbirliği yapabilmek ve bulut üzerinden kuantum hesaplamanın gerçekleştirilebilmesi için bir ortam oluşturmaktır [6]. D-Wave'in yüksek kübite sahip kuantum bilgisayarları optimizasyon problemlerinin çözümünde kullanılmaktadır [7].

Tablo 4.1. Günümüz Kuantum Bilgisayarları

Şirket	Teknoloji	Kubit
Intel	Süper iletkenler (Kapı)	49
Google	Süper iletkenler (Kapı)	72
IBM	Süper iletkenler (Kapı)	50
D-Wave	Süper iletkenler (Kuantum sertleşmesi)	2048
Intel-qHiPSTER	Klasik (Simülatör)	43
IBM Research	Klasik (Simülatör)	56
Microsoft Azure	Klasik (Simülatör)	40

Günümüzde güvenilir olarak kullanılan asimetrik sistemler ayrık logaritma veya çarpanlarına ayırma problemine dayanmaktadır. Bu problemler klasik bilgisayarlarda hesaplama gücünün yetersizliğinden dolayı polinom zamanda çözülememektedir. 1994 yılında Peter Shor, klasik bilgisayarlarda ayrık logaritma ve çarpanlarına ayırma gibi hesaplamalı zor problemleri kuantum bilgisayarlarda polinom zamanda çözebilecek bir algoritma önermiştir [8]. Shor'un önerdiği algoritma ile kuantum bilgisayarlarda günümüz açık anahtarlı kriptosistemlerin dayandığı çarpanlarına ayırma veya ayrık logaritma gibi zor problemlerin çözülecek olması açık anahtarlı kriptosistemler için

tehdit oluşturmaktadır. Bu sebepten, kuantum sonrasında güvenilir bir şekilde kullanılabilecek kriptosistemlere ihtiyaç vardır. NIST (Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü - National Institute of Standards and Technology) yayınladığı raporda günümüzdeki sistemlerde güvenilir bir şekilde kullanılan RSA, DSA, ECDSA gibi açık anahtarlı kriptosistemlerin kuantum hesaplayıcıların ortaya çıkmasından sonra güvensiz hale geleceğini ifade etmiştir [9]. Tablo 4.2 'de günümüzde kullanılan simetrik ve asimetrik kriptosistemler, kullanım amaçları, kuantum öncesinde sağladıkları güvenlik seviyeleri, bu kriptosistemlerin kuantum bilgisayarlar sonrasındaki güvenlik seviyeleri ile kuantum bilgisayarlarda bu kriptosistemleri kırmak için gerekli olan yaklaşık kübit sayıları verilmektedir [9],[10], [11].

Tablo 4.2. Kuantum Sonrasında Kriptosistemlerin Güvenlik Seviyeleri

Kriptosistem	Tip	Amaç	Güvenlik Seviyesi	Kuantum Sonrasındaki Güvenlik Seviyesi	Kriptoistemi Kırmak için Gereken Kübit Sayısı*
AES-128	Simetrik	Şifreleme	128-bit	64-bit (Grover alg.)	-
AES-256	Simetrik	Şifreleme	256-bit	128-bit (Grover alg.)	-
SHA-256	-	Özet Fonksiyonu	256-bit	128-bit (Grover alg.)	-
RSA (n-bit)	Asimetrik	Şifreleme İmzalama Anahtar Değişimi	128-bit	0-bit (Shor alg. ile kırıldı)	$2n$
DH/DSA (n-bit)	Asimetrik	İmzalama Anahtar Değişimi	128-bit	0-bit (Shor alg. ile kırıldı)	$2n$
Curve25519 (n-bit)	Asimetrik	Şifreleme İmzalama Anahtar Değişimi	128-bit	0-bit (Shor alg. ile kırıldı)	$6n$
ECDH/ECDSA (n-bit)	Asimetrik	İmzalama Anahtar Değişimi	128-bit	0-bit (Shor alg. ile kırıldı)	$6n$

* Kuantum bilgisayarlarda kriptosistemi kırmak için ihtiyaç duyulan yaklaşık kübit sayısı

Tablo 4.2 'de kuantum bilgisayarlar ile asimetrik kriptosistemlerin güvensiz olduğu ifade edilmiş ve kuantum bilgisayarda kriptosistemleri kırmak için yaklaşık olarak kaç kübite ihtiyaç duyulduğu verilmiştir. Örneğin RSA-2048'i kırmak için yaklaşık $2 \times 2048 = 4096$ kübit gerekmektedir. Benzer şekilde Curve25519 parametrelerini kullanan eliptik eğri sisteminde anahtarın bit sayısı 255'dir. Bu durumda bu kriptosistemi kuantum bilgisayarda

çözebilmek için yaklaşık $6 \times 255 = 1530$ kübite ihtiyaç bulunmaktadır.

Büyük şirketler tarafından kuantum bilgisayarların üretildiğini ve kuantum algoritmalar ile günümüz kriptosistemlerin dayandığı hesaplamalı zor problemlerin güvensiz hale geldiğini bilmekteyiz. Kuantum araştırma merkezinde araştırmacı olarak çalışan Mosca 2015 yılında yaptığı konuşmada RSA-2048'in 1/7 olasılıkla 2026 yılına kadar ve 1/2 olasılıkla 2031 yılına kadar kırılacağını öngördüğünü söylemiştir [12]. Kuantum sonrası için kriptosistemlerin oluşturulması ve standartlaşma süreci için çalışmalar yapılmaktadır. Ancak kuantum sürecine birden bire geçilemeyeceği de açıktır. Var olan kriptosistemlerin belli bir süre kullanılması gerekecektir. Bunun yanı sıra, RSA, DSA, ECDSA gibi günümüzde kullanılan asimetrik kriptosistemlerin kuantum bilgisayarlara karşı dirençli hale getirilmesi mümkün değildir. Mosca bu konuda çözüm önerilerinde bulunmuştur [12]. Çarpanlarına ayırma veya ayrık logaritma problemi haricinde matematiksel problemlere dayanan ve kuantum ataklara karşı güvenilir olduğu bilinen klasik şifreleme yöntemlerini kullanarak kriptosistemlerin oluşturulması önerilmektedir. Kuantum geçiş sürecinde, kriptosistemlerin anahtar boyutları arttırılarak ve var olan kriptosistemlerden hibrit sistemler elde edilerek geçici çözümler oluşturulabilir. Kuantum geçiş sürecinde kritik öneme sahip şifreleme cihazlarındaki anahtar paylaşımı ve yönetiminin kuantum bilgisayarlara karşı dirençli bir hale getirilmesi, simetrik şifreler için anahtar boyutlarının kuantum güvenlik düzeyine gelebilmesi için artırılması ve kritik bilgilerin en kısa sürede kuantum bilgisayarlara karşı dirençli sistemler ile yeniden şifrelenmesi, imzalanması oldukça önemlidir.

Yukarıda bahsedilenler ve Tablo 4.2 dikkate alındığında, kırılan asimetrik kriptosistemlerin yerine kuantum sonrasında kullanılabilecek güvenilir şifreleme, kimlik doğrulama, imzalama ve anahtar değişimi amacıyla kullanılabilecek kriptosistemlerin oluşturulması gerekmektedir. Konuya dikkat çekerek kriptosistemlerin oluşturulması ve bir sonraki aşamada bu sistemlerin standartlaştırılması amacıyla NIST 2016 yılında

Kuantum Sonrası Kriptografi Standartlaştırma Projesi (Post-Quantum Cryptography Standardization Project) ismiyle bir çağrıya çıkmıştır. Bu çağrının ilk aşaması 2018 yılı itibariyle tamamlanmıştır. NIST, kuantum ve klasik bilgisayarların saldırılarına karşı dirençli olduğu bilinen kriptosistemlere dayanan farklı kriptosistemleri ilk aşama gönderileri olarak yayınlamıştır. NIST'in kuantum sonrası için yaptığı bir başka çalışma ise kuantum bilgisayarlarda çalışan algoritmaların bir araya getirilmesidir. NIST, klasik bilgisayarlarda polinom zamanda çözülemeyen problemleri, kuantum bilgisayarlarda (polinom zamanda) çözen algoritmaları `Quantum Algorithm Zoo' web sayfasında bir araya toplamaktadır [13]. Ayrıca, klasik algoritmaların karmaşıklıkları ile aynı problemi çözen kuantum algoritmaların karmaşıklıklarını karşılaştırmaktadır.

4.1.1. Motivasyon

Kuantum bilgisayarların ortaya çıkması ile açık anahtarlı kriptosistemler güvensiz hale gelecektir. Bu nedenle kırılan kriptosistemlerin yerine kuantum ataklara karşı dirençli kriptosistemlerin oluşturulmasına ihtiyaç vardır. Zorluğu çarpanlara ayırma veya ayrık logaritma problemine dayanan kriptosistemleri güvensiz hale getiren Shor algoritması ve simetrik kriptosistemlerin güvenlik düzeyinin düşmesine neden olan Grover algoritmasının temel adımlarının detaylandırılması ve uygulama odaklı olacak bir şekilde ifade edilmesinin önemi büyüktür. Ayrıca, kuantum bilgisayarlar sonrası güvenilir kriptosistem sınıfları hakkında bilgi verilmesi ve kuantum hesaplayıcılar sonrasında problemlerin zorluk düzeylerinin yeniden belirlenmesi üzerine yapılan çalışmalara eklemeler yapılmasına ihtiyaç vardır. Bu kapsamda, çok değişkenli polinom sistemlerine dayanan kimlik doğrulama sistemleri ayrı bir ilgi görmektedir.

4.1.2. Organizasyon

Çalışmanın devam eden kısmı şu şekilde organize edilmiştir. Bölüm 4.2 'de kuantum algoritmalardan olan Shor ve Grover algoritmalarına yer verilmektedir. Shor ve Grover algoritmalarının

hangi problemleri çözdüğü açıklanarak algoritmanın adımları ele alınmaktadır. Bölüm 4.3 'te kuantum sonrası için güvenilir kriptosistem sınıflarından biri olan çok değişkenli polinom sistemi ve çok değişkenli polinom sistemlerinin dayandığı zor problem için temel tanımlar verilmektedir. Bölüm 4.4 'te kuantum sonrasında kullanılabilecek kriptosistem sınıfları anlatılmaktadır. Çok değişkenli polinom sistemlerine dayanan kimlik doğrulama ve imzalama şemalarına yer verilmektedir. Son bölümde ise sonuçlar ve gelecek çalışmalar ifade edilmiştir.

4.2. Kuantum Bilgisayarlar İle Kriptoanaliz Algoritmaları

Klasik bilgisayarlar, RSA, DSA ve ECDSA gibi kriptosistemlerin dayandığı zor problemleri polinom zamanda çözebilecek hesaplama gücüne sahip değildir. Ancak bu kriptosistemlerin dayandığı zor problemleri kuantum bilgisayarlarda polinom zamanda çözebilen kuantum algoritmalar mevcuttur. Bu algoritmalardan Shor ve Grover algoritmalarına bu bölümde yer verilmiştir.

4.2.1. Shor Algoritması

Peter W. Shor tarafından önerilen bu algoritma kuantum bilgisayarlarda çok büyük sayıları bile polinom zamanda çarpanlarına ayırabilmektedir. Açık anahtarlı kriptografide yaygın olarak kullanılan RSA kriptosistemin güvenliği büyük sayıları çarpanlarına ayırmanın zorluğuna dayanmaktadır. Bu bakımdan, Shor algoritması klasik kriptografiden kuantum sonrası yapıya geçmeye neden olması açısından önemlidir. Çarpanlarına ayırma problemi, birbirinden farklı p ve q asal sayılarının çarpımından oluşan $N = p \times q$ sayısı verildiğinde, bu N sayısının asal çarpanlarını elde etme problemi olarak tanımlanmaktadır. Shor algoritmasında, bu çarpanları elde etmek için periyodik bir fonksiyona ihtiyaç olmaktadır. $x < N$ ve x ile N aralarında asal olmak üzere $F(a) = x^a mod(N)$ periyodik bir fonksiyon olsun. $F(a)$ periyodu r olan periyodik bir fonksiyon ise $F(a + r) = F(a)$ olmalıdır. Shor algoritması, verilen bir N sayısı için $F(a) = x^a \, mod(N)$ fonksiyonunun periyodunu bulunmaktadır. Sonra

bulunan periyot kullanılarak N sayısı çarpanlarına ayrılmaktadır [8].

Klasik bilgisayarlarda çarpanlarına ayırma işlemi için bilinen en verimli algoritmanın karmaşıklığı $O(e^{(logN)^{1/3}(loglogN)^{2/3}})$'dir [14]. Bunun yanı sıra, bit sayısı 1000 veya daha fazla olduğunda klasik bilgisayarlar ve bilinen algoritmalar kullanılarak sayıyı makul sürelerde çarpanlarına ayırmak mümkün değildir. Oysa, Shor algoritması polinom zamanlıdır, daha açık ifadeyle $O(logN^3)$ çalışma zamanına sahiptir [14]. Shor algoritması, kuantum bilgisayarlarda periyot bulma problemini gerçekleştiren kuantum algoritmalar ile klasik bilgisayarlarda yürütülen algoritmalar olmak üzere iki kısımdan oluşmaktadır. Shor algoritması için çok büyük önem arzeden kuantum Fourier dönüşümü Tanım 4.1 'de verilmektedir.

Tanım 4.1. (Kuantum Fourier Dönüşümü (Quantum Fourier Transform-QFT)): Kuantum Fourier dönüşümü, ayrık Fourier dönüşümünün bir çeşididir [15], [16].

Hatırlatma: $x = (x_0, x_1, \dots, x_N)$ dönüşüm uygulanacak vektör olmak üzere ayrık Fourier dönüşümü:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i j k/N} \tag{1}$$

Kuantum Fourier dönüşümünün ayrık Fourier dönüşümünden tek farkı x ve y durum vektörleridir. x ve y durum vektörleri:

$$x = \sum_{j=0}^{N-1} x_j |j\rangle \tag{2}$$

$$y = \sum_{j=0}^{N-1} y_j |j\rangle \tag{3}$$

x durum vektörü için kuantum Fourier dönüşümü:

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} x_j \, e^{2\pi i j k/N} \, |k\rangle \tag{4}$$

şeklinde ifade edilmektedir. Algoritma 4.1 'de Shor algoritmasının hem klasik hem de kuantum bilgisayarlarda yürütülen adımları verilmiştir [8], [14], [17].

Algoritma 4.1: Shor Algoritması

1) $N = p \times q$ sayısının çift sayı, asal sayı ya da asal sayının kuvveti olup olmadığı kontrol edilir. Eğer öyleyse Shor algoritması kullanılamaz. Bu adım klasik bilgisayarlarda yapılacaktır.
2) $x < N$ olacak şekilde bir x tamsayısı seçilerek
$$d = \gcd(x, N) \begin{cases} 1, & x \text{ ile } N \text{ aralarında asaldır.} \\ aksi\ halde, & d = p \text{ veya } d = q \end{cases}$$
Bu adım klasik bilgisayarlarda yapılacaktır.
3) $N^2 \leq q = 2^l < 2N^2$ olacak şekilde 2'nin kuvveti olan bir q sayısı seçilir.
4) Kuantum kaydedici seçilir. Kaydedici 1 ve Kaydedici 2 olmak üzere ikiye ayrılır. Kuantum bilgisayarda bu kaydediciler $|reg1, reg2\rangle$ olacak şekilde gösterilecektir.

   Giriş kaydedicisi olarak kullanılan Kaydedici 1, $(q-1)$ 'e kadar olan sayıları kaydedebilmek için gerekli olan $log_2 q$ kübitlik bir kaydedicidir.

   Çıkış kaydedicisi olarak kullanılan Kaydedici 2 ise $(N-1)$'e kadar olan sayıları kaydedebilmek için gerekli olan kübite sahip bir kaydedicidir.
5) Kaydedici 1'e, 0'dan $(q-1)$'e kadar olan sayıların eşit ağırlıklı süperpozisyonu kaydedilir. Kaydedici 2'ye ise sıfır yazılır. Bu işlem kuntum bilgisayarlarda yapılacaktır. Kuantum bilgisayarlarda kaydedicilerin durumu
$$\underbrace{\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a,}_{Kaydedici\ 1} \underbrace{0\rangle}_{Kaydedici\ 2}$$
şeklinde gösterilecektir.
6) Kaydedici 1'de kayıtlı olan 0'dan $(q-1)$'e kadar her sayı için $x^{|a\rangle}(modN)$ dönüşümü yapılır. 0 değerleri atanmış olan Kaydedici 2'ye dönüşüm sonuçları yazılır. Kaydedici 1'deki her sayı için $x^{|a\rangle}(modN)$ değeri hesaplandıktan sonra kaydediciler

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a, x^a\ (mod\ N)\rangle$$

yukarıda verildiği gibi olacaktır.

7) Bu adımda Kaydedici 1'e Kuantum Fourier dönüşümü (QFT) uygulanır. Bu durumda Kaydedici 1'in değeri:

$$\left|a\rangle = \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1} e^{2\pi iac/q}\right| c\rangle$$

eşitliği ile hesaplanır. QFT uygulandıktan sonra kaydedicilerin durumu

$$\frac{1}{q}\sum_{a=0}^{q-1}\sum_{c=0}^{q-1} e^{2\pi iac/q}\,|c\rangle\,|x^a\ (mod\ N)\rangle$$

şeklinde olacaktır.

8) Kaydedicilerdeki $|c\rangle$ ve $|x^a(modN)\rangle$ durumları için ölçümler yapılır. Örneğin $x^a = x^k$ eşitliğini sağlayan bir k değeri bulup makinenin $|c, x^k(modN)\rangle$ durumu için durma olasılığı:

$$\frac{1}{q}\left|\sum_{a:x^a\equiv x^k} e^{2\pi iac/q}\right|^2$$

olarak hesaplanır. r, x'in periyodunu ifade etmek üzere a, $a \equiv k(mod\ r)$'yı sağlayan bütün değerlerin toplamıdır. Bu sebepten, $a = br + k$ olarak yazabilir ve $|c, x^k(mod\ N)\rangle$ durumunun olasılığı:

$$p(c) = \frac{1}{q}\left|\sum_{b=0}^{q-k-1} e^{2\pi i(br+k)c/q}\right|^2$$

gibi olacaktır. $p(c)$ için ilgili hesaplama yapıldığında olasılık hesabının $-r/2 < rc - dq \leq r/2$ şartına bağlı olduğu görülür. Verilen şart rq'a bölünürse $\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}$ eşitsizliği elde edilmektedir. c ve q değerleri bilindiğinden eşitsizliği sağlayacak en fazla bir d değeri vardır. c/q değerine sürekli kesir açılımı (continued fraction expansion) yapılarak d ve aralarında asal olacak şekilde

d/r değeri bulunabilir. Belirlenen r periyodu çift sayı ve $x^{r/2} mod N \neq -1$ olana kadar periyod bulma işlemine devam edilir. Bu adım sonunda Shor algoritmasının kuantum bilgisayarlarda gerçekleştirilen periyod bulma problemi tamamlanmış olmaktadır.

9) Klasik bilgisayarlarda Öklit algoritması kullanılarak $d = max\{\gcd(x^{r/2} - 1, N), \gcd(x^{r/2} + 1, N)\}$ ortak bölenlerin en büyüğü (greatest common divisor-gcd) hesaplanır. Eğer $d = 1$ ise 4. adıma geri dönülür aksi halde, $d \neq 1$ ise bulunan değer N sayısının çarpanlarının en büyüğüdür.

Literatürde 15 sayısının çözümü üzerine birçok örnek yer almaktadır. Örneğin, IBM tarafından geliştirilen IBM Q Experience kuantum simülatöründe $N = 15$ sayısının çarpanlarına ayrılması için örnek kodlar mevcuttur [18]. Simülatörde kuantum algoritmalarında kullanılan kuantum kapılar ve operatörler hazır olarak verilmektedir. Örnek 4.1.'de Shor algoritmasının 21 sayısını çarpanlara ayırmak için çalıştırdığımız zaman yapılacak adımlar gösterilmiştir.

Örnek 4.1. $N = 21$ sayısını Shor algoritmasını kullanarak çarpanlarına ayıralım.

- İlk adımda çarpanlarına ayrılmak istenen sayı kontrol edilir. $N = 21$ çift sayı, asal sayı veya asal sayının kuvveti olmadığı için $N = 21$ Shor algoritması kullanılarak çarpanlarına ayrılabilir.
- $1 < x < N$ olacak şekilde rastgele x tamsayısı seçelim.
    - Örneğin; seçilen sayı $x = 6$ ise $\gcd(6,21) = 3$ olur ve çarpanlardan biri bulunur.
    - $x = 11$ ise 11 ile 21 aralarında asal iki sayı ve $\gcd(11,21) = 1$ olduğundan bir sonraki adıma geçilir.
- $21^2 \leq q = 2^l < (2.21)^2 = 882$ olacak şekilde bir q sayısı seçilir. $q = 512 = 2^9$ olarak seçelim.
- Kaydedici 1 ve Kaydedici 2 sıfır (0) başlangıç değeri ile set edilir.

$$|\phi_i = |0\rangle_{r_1}|0\rangle_{r_2} = 0\rangle^{\otimes 2^l}$$

- Kaydedici 1'e 0'dan $(q-1)$'e kadar olan sayıların eşit ağırlıklı süperpozisyonu kaydedilir. Kaydedici 2'de hala sıfır yazmaktadır.

$$\frac{1}{\sqrt{512}}\sum_{a=0}^{511}|a\rangle, |0\rangle$$

Hatırlatma: Kuantum bilgisayarlar kübitlerle işlem yapmaktadır. Kübitler süperpozisyon özelliğine sahip olduğundan bütün kübitler $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ olacak şekilde iki durumun toplamı olarak ifade edilir.

- Bütün durumlar için $x^{|a\rangle}(modN)$ değerlerinin süperpozisyonu Kaydedici 2'ye yazılır.

$$\frac{1}{\sqrt{512}}\sum_{a=0}^{511}|a, 11^a \bmod 21\rangle = \frac{1}{\sqrt{512}}(|0\rangle|1\rangle + |1\rangle|11\rangle + |2\rangle|16\rangle + |3\rangle|8\rangle + |4\rangle|4\rangle + \cdots + |511\rangle|11\rangle)$$

$11^a(mod\ 21)$ için elle hesaplama yapılırsa:

a	0	1	2	3	4	5	6	7	8	9	10	…	511
$11^a(mod\ 21)$	1	11	16	8	4	2	1	11	16	8	4	…	11

- Kaydedici 1'e QFT uygulanır.

$$\frac{1}{512}\sum_{a=0}^{511}\sum_{c=0}^{511} e^{2\pi iac/512}|c\rangle 11^a(mod\ 21)\rangle$$

- Kaydedicilerin durumları $|c\rangle$ ve $|11^a(mod 21)\rangle$ için ölçülür. Örneğin; $k=2$ için $|c, 11^2\ mod\ 21\rangle \rightarrow |c, 16\rangle$ işlemi sonunda kaydedicilerin durumunun olasılığı (probability):

$$P(c) = \left|\frac{1}{512}\sum_{a:11^a\ mod\ 21=16}^{511} e^{2\pi iac/512}\right|^2 = \left|\sum_b e^{2\pi i(6b+2)c/512}\right|^2$$

- Bu aşamada kuantum bilgisayarda periyoda karar verme işlemi yapılmaktadır. c = 427 olarak alınırsa $\left|\frac{427}{512} - \frac{d}{r}\right| \leq \frac{1}{2.512}$ eşitsizliği sağlanmalıdır. Sürekli kesir açılımı yapılırsa:

$$\frac{c}{q} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots}}} = \frac{p_n}{q_n}$$

$$\frac{427}{512} = 0 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{42 + \cfrac{1}{1 + \frac{1}{1}}}}}$$

Sürekli kesir açılımındaki a_n, p_n, q_n'nin değerleri $n = 0,1,2,3, \ldots$ için tabloda verilmiştir.

n	0	1	2	3	4	5
a_n	0	1	5	42	1	1
p_n	0	1	5	211	216	427
q_n	1	1	6	253	259	512

$11^{q_n} = 1 \; mod \; 21$ olacak şekilde yukarıdaki tablodan $q_n = r$ değeri bulunur. $n = 0$ ve $n = 1$ durumları şartı sağlamamaktadır. $n = 2$ için $q_n = 6$ olur ve $11^6 = 1 \; mod \; 21$'dir. Bulunan $r = 6$ periyodunun çift sayı ve $11^{6/2} \; mod \; 21 \neq -1$ olup olmadığı kontrol edilir. Şartları sağladığından periyot belirlenmiş olur.

- Son adımda Öklid algoritması kullanılarak:

$$x^{r/2} mod \; N - 1 = \; 11^3 \; mod \; 21 - 1 = 7 x^{r/2} \; mod \; N + 1$$
$$= 11^3 \; mod \; 21 + 1 = 9$$

21 sayısının ikinci çarpanı $\gcd(7,21) = 7$ bulunmuş olmaktadır.

4.2.2. **Grover Algoritması:**

Grover algoritması, verilen N elemanlı sırasız veri içerisinde istenilen elemanı bulmak için kullanılan bir arama algoritmasıdır [19]. Klasik bilgisayarlarda sıralı olmayan veri içerisinden bir elemanı aramak için en basit yöntem doğrusal aramadır. Bu yöntem ile N elemanlı bir veride istenilen elemanı bulmanın maliyeti $O(N)$'dir. Bunun yanı sıra, Grover algoritması bu arama işlemini $O(\sqrt{N})$ zaman karmaşıklığında yapmaktadır. Bu bakımdan Grover algoritması arama problemine önemli bir hız

kazandırmaktadır. Kübitlerin süperpozisyon özelliğine sahip olması Grover algoritmasının arama işlemini böyle bir hızda gerçekleştirmesini sağlamıştır.

Tanım 4.2. (Arama Problemi): $N = 2^n$ olsun. Burada, n kuantum bilgisayarda N boyutlu arama uzayını gösterebilmek için ihtiyaç duyulan kübit sayısını göstermektedir. $x = \{x_1, x_2, \dots, x_N\}$ sıralanmamış kümesi içerisinden istenilen elemanı bulan fonksiyon

$$f(x) = \begin{cases} 0, & 0 < x \leq 2^n \\ 1, & x = x_0 \end{cases}$$

olarak tanımlansın. Arama probleminde amacımız $f(x) = 1$ olacak şekilde $x = x_0$ elemanını bulmaktır.

Kuantum bilgisayarda çalıştırılan Grover algoritmasının adımları Algoritma 4.2 'de verilmiştir [20], [21].

Algoritma 4.2: Grover Algoritması

1) $N = 2^n$ elemanlı bir veri üzerinde arama yapabilmek için ilk olarak n kübitlik bir kuantum kaydediciye başlangıç değeri atanır.
$$|0\rangle^{\otimes n} = |0\rangle$$
Bu adımın sonunda kaydedicideki her kübit 0 değerini alır.
2) Bütün kübitlere Hadamard dönüşümü uygulanır. Bu sayede kübitler eşit süperpozisyon durumundadır.
$$|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$
3) Bu adımda Grover iterasyonları adı verilen bir dizi işlem yapılır. Bu adımda yapılan ilk işlem $\mathcal{O}$ kuantum kahini (quantum oracle) çağırmaktır. $\mathcal{O}$ kuantum kahini, $|x\rangle$ değerlerini alan aşağıdaki gibi tanımlanmış bir fonksiyondur:
$$\mathcal{O}|x\rangle = (-1)^{f(x)}|x\rangle \qquad (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle, f(x) = 0 \\ -|x\rangle, f(x) = 1 \end{cases}$$

ψ bir önceki adımda hesaplanan tüm kübitlerin süperpozisyonunu göstermek üzere Grover operatörü G:

$$G = (2|\psi\rangle\langle\psi| - I)\mathcal{O}$$

olarak tanımlanmaktadır. Grover operatörü $R \approx \frac{\pi}{4}\sqrt{2^n}$ defa tekrarlanır. Bu iterasyonlar sonucunda aranan eleman bulunmaktadır.

$$[(2|\psi\rangle\langle\psi| - I)\mathcal{O}]^R|\psi\rangle \approx |x_0\rangle$$

4) Bu adımda aranan eleman olan x_0'ın değeri okunur.

4.3. Matematiksel Altyapı

Bu bölümde çok değişkenli polinom sistemleri ile ilgili tanımlara yer verilmektedir. Bu bölümdeki tanımların anlaşılabilmesi çok değişkenli polinomlara dayanan kriptosistemlerin oluşturulabilmesi açısından önemlidir. Tanım 4.3 'te sonlu cisim tanımı yapılmıştır.

Tanım 4.3. (Sonlu Cisim): Sonlu sayıda elemanı olan cisim sonlu cisim olarak adlandırılmaktadır [22]. $\mathbb{F}$, sonlu sayıda elemanı olan sonlu bir cismi gösterirken; q, asal sayı veya asal sayının kuvveti olmak üzere q elemanlı bir sonlu cisim $\mathbb{F}_q$ ile gösterilmiştir. $\mathbb{F}_q^n$ ise elemanları 0 ile $q-1$ arasında olan q elemanlı sonlu cisimde n boyutlu vektör uzayını temsil etmektedir.

Kuantum sonrası kriptografide kullanılan çok değişkenli polinom sistemleri sonlu cisimler üzerine tanımlanmıştır. Tanım 4.4.'te çok değişkenli polinom sistemleri ele alınmaktadır.

Tanım 4.4. (Çok Değişkenli Polinom Sistemi): $\mathbb{F}_q^n$ sonlu cisminde n değişkenli d. dereceden m tane polinomdan oluşan F çok değişkenli polinom sistemi, $(f_{i\ldots j}^{(k)}, f_i^{(k)}$ ve $f_0^{(k)}, 1 \leq k \leq m$ olmak üzere Eşitlik (5)'teki gibi tanımlanmaktadır [23].

$$
\begin{aligned}
f^{(1)}(x_1,\ldots,x_n) &= \sum_{i}^{n}\cdots\sum_{j}^{n} f_{i\ldots j}^{(1)}\cdot\overbrace{x_i\cdot\ldots\cdot x_j}^{d}+\ldots+\sum_{i=1}^{n} f_i^{(1)}\cdot x_i + f_0^{(1)}\\
f^{(2)}(x_1,\ldots,x_n) &= \sum_{i}^{n}\cdots\sum_{j}^{n} f_{i\ldots j}^{(2)}\cdot\overbrace{x_i\cdot\ldots\cdot x_j}^{d}+\ldots+\sum_{i=1}^{n} f_i^{(2)}\cdot x_i + f_0^{(2)}\\
&\vdots\\
f^{(m)}(x_1,\ldots,x_n) &= \sum_{i}^{n}\cdots\sum_{j}^{n} f_{i\ldots j}^{(m)}\cdot\overbrace{x_i\cdot\ldots\cdot x_j}^{d}+\ldots+\sum_{i=1}^{n} f_i^{(m)}\cdot x_i + f_0^{(m)}.
\end{aligned}
\tag{5}
$$

Kullanılan polinomların derecesi $d = 2$ ve $d = 3$ olarak alınırsa sırasıyla ikinci dereceden (MQ) ve üçüncü dereceden (MC) çok değişkenli polinom sistemi elde edilmektedir. Bu alanda yapılan çalışmalara baktığımızda verimlilik açısından ve hesaplama anlamında daha kolay olduğundan genellikle ikinci dereceden çok değişkenli polinom sistemleri kullanılmıştır. Tanım 4.5 'te çok değişkenli polinomlara dayanan sistemlerin dayandığı kuantum sonrasında da polinom zamanda çözülemeyen zor problem tanımlanmıştır.

Tanım 4.5. (Çok Değişkenli Problem): Eşitlik (5)'te verilen m tane polinom $(f^{(1)}(x),\ldots,f^{(m)}(x))$ için $f^{(1)}(\bar{x}) = \cdots = f^{(m)}(\bar{x}) = 0$ olacak şekilde $\bar{x} = \bar{x}_1,\ldots,\bar{x}_n$ değerlerinin bulunup bulunamayacağı çok değişkenli problem olarak tanımlanmıştır. Başka bir ifadeyle, çok değişkenli problemin zorluğu, sonlu bir cisimde F polinom sistemi için $F(x) = 0$ yapan x değerlerini bulmanın zor olmasına dayanmaktadır [23]. Bu problem hem klasik bilgisayarlarda hem de kuantum bilgisayarlarda polinom zamanda çözülemediğinden NP-zor bir problemdir.

İkinci dereceden polinom sistemlerinin dayandığı zor problem literatürde MQ problem olarak bilinmektedir. MQ problemin çözümünün zorluğunun parametre değerlerine, özellikle değişken sayısına, denklem sayısına ve sonlu cisim uzayına bağlı olduğu belirtilmiştir. Tablo 4.3 'te ikinci dereceden çok değişkenli polinom sistemlerinin hangi durumlarda kuantum sonrası zor problem

olarak adlandırılabileceklerine yönelik parametre karşılaştırmaları bulunmaktadır [24].

Tablo 4.3. $\boldsymbol{MQ}$ polinom sistemleri için parametreler

Grup I :	Şifreleme,	$m = 2n$	$\mathbb{F}_2$
Grup II :	Şifreleme,	$m = 2n$	$\mathbb{F}_{2^8}$
Grup III :	Şifreleme,	$m = 2n$	$\mathbb{F}_{31}$
Grup IV :	İmzalama,	$n \approx 1.5\, m$	$\mathbb{F}_2$
Grup V :	İmzalama,	$n \approx 1.5\, m$	$\mathbb{F}_{2^8}$
Grup VI :	İmzalama,	$n \approx 1.5\, m$	$\mathbb{F}_{31}$

Çok değişkenli problemdeki değişken sayısıyla denklem sayısı birbirine eşit olsa bile bu problem kuantum bilgisayarlarda polinom zamanda çözülemediğinden çok değişkenli polinom sistemleri kullanılarak oluşturulan kriptosistemler kuantum ataklara karşı dirençli olmaktadır. Bu sebepten, kuantum sonrasında çok değişkenli polinom sistemlerine dayanan şifreleme, imzalama ve kimlik doğrulama için önerilen birçok kriptosistem mevcuttur.

Kuantum bilgisayar ataklarına karşı dirençli kriptosistemlerin oluşturulması gerektiği bilmekteyiz. Bu kapsamda kuantum sonrası güvenilir kriptosistemlerin oluşturulması için yapılması gerekenler şu şekilde özetlenebilir:

- Kuantum bilgisayarlarda bile polinom zamanda çözülemeyen zor problemlerin bulunması,
- Güvenliği, seçilen zor problemin çözülememesine dayanan kriptografik algoritma/protokol oluşturulması,
- Oluşturulan algoritma/protokol için güvenlik analizinin teorik ve uygulamalı olarak gerçeklenmesi,
- Kullanılacak mimariye göre güvenlik analizlerinin yapılması,

- Farklı güvenlik seviyeleri için algoritma/protokol parametrelerinin belirlenmesi ve bu parametreler için güvenlik analizlerinin yapılması,
- Hedef platformda algoritmanın verimli bir şekilde çalışabilmesi için güncellemelerin yapılması.

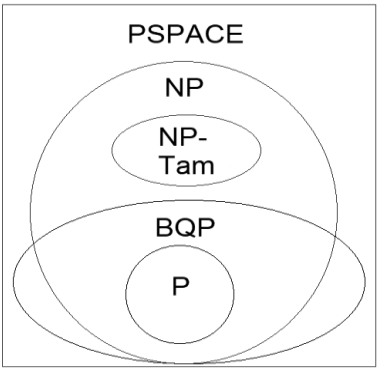
4.4. Kuantum Sonrası Kriptosistem Sınıfları

Bu bölümde kuantum bilgisayarlarda bile polinom zamanda çözülemeyen problemlere dayanan kriptosistemler ele alınmaktadır. Kuantum bilgisayarlardan sonra oluşan problem sınıflarına yer verilmiştir. Çok değişkenli polinomlara dayanan kimlik doğrulama ve imzalama şemaları üzerinde durulmuştur.

Açık anahtarlı kriptografinin dayandığı zor problemlerden biri olan çarpanlarına ayırma probleminin Shor tarafından önerilen bir algoritma ile kuantum bilgisayarlarda çözülmesi, kuantum kriptografi adında yeni bir bilim dalının ortaya çıkmasına neden olmuştur. Bunun yanında, kuantum bilgisayarlar ile hesaplama gücünün artması ve klasik kriptografinin dayandığı zor problemlerin kuantum bilgisayarlarda çözülmesi gibi sebepler kuantum bilgisayarlarda bile kırılmayacak kriptosistemlerin araştırılması gerekliliğini doğurmuştur. NIST'in bu konuda yaptığı çağrının da etkisiyle çalışmalar hem kuantum hem de klasik bilgisayarlara karşı dirençli sistemlere yönelmiştir. Bu sebepten, oluşturulacak kriptosistemin güvenliği temelindeki matematiksel problemlerin zorluğuna dayanmaktadır. Bu bakımdan, sistemin dayandığı matematiksel problemin hangi problem sınıfında olduğu önemlidir.

Kuantum sonrası güvenli kriptosistem tasarımı için gerekli olan zor problemler, klasik bilgisayarlarda ve kuantum bilgisayarlarda polinom zamanda çözülemeyen problemler olarak tanımlanabilir. Klasik bilgisayarlarda polinom zamanda çözülemeyen problemler NP (nonpolynomial-time) sınıfını oluşturmaktadır. Klasik bilgisayarlarda NP sınıfta olan birçok problem kuantum bilgisayarlarda polinom zamanda çözülerek P sınıfına indirgenmektedir. Bu sebepten, NP sınıfında olan problemler kuantum bilgisayarlarda polinom zamanda çözülebilen BQP

sınıfını oluşturacaktır [20]. Şekil 4.1 'de kuantum bilgisayarlar sonrasında oluşacak problem sınıfları gösterilmektedir. Burada kuantum sonrası güvenli kriptosistem tasarımı için bakacağımız problem sınıfı NP-tam ailesindedir.



Şekil 4.1. Kuantum sonrasında problem sınıflarının gösterimi

Kuantum sonrası kriptografinin amacı, kuantum bilgisayarlarda bile polinom zamanda çözülemeyecek NP sınıfında olan zor problemlere dayanan kriptosistemler oluşturabilmektir. Kuantum bilgisayarlarda kafes, çok değişkenli polinomlar, kod, özet fonksiyonları ve izojeni tabanlı kriptosistemleri polinom zamanda çözebilecek bir algoritma henüz önerilmemiştir [9], [23]. Dolayısıyla bu zor problemlere dayanan sistemler kuantum sonrası için oluşturulmaya başlanmıştır. Bu bölümde kuantum sonrası kriptografi için önerilen kriptosistem aileleri özetlenecektir.

NIST'in kuantum bilgisayarlara karşı güvenilir kriptosistemlerin oluşturulması amacıyla başlattığı çağrı hakkındaki bazı bilgilere giriş bölümünde yer verilmişti. Bu çağrıda, kuantum sonrasında kullanılabilecek kriptosistemlere ihtiyaç olduğu vurgulanmıştır. Bu nedenle, çağrıya kuantum bilgisayarlara karşı güvenilir yeni şifreleme, imzalama ve anahtar değişim algoritmaları gönderilmiştir. NIST'in düzenlediği bu çağrıya istenenleri sağlayacak şekilde gönderilen 69 algoritma Tablo 4.4 'te verilmektedir [25]. NIST'in amacı gönderilen algoritmalardan kuantum ataklara karşı dirençli olanları seçerek kuantum sonrası için standartlaşma sürecini başlatabilmektir [9]. NIST, 30 Ocak

2019 tarihinde bu çağrıya gönderilen algoritmalardan belli kriterlere göre seçtiği algoritmaları açıklamıştır. Tablo 4.4 'te ikinci aşamaya kalan algoritmaların isimleri altı çizili olarak ifade edilmektedir.

Kuantum sonrası güvenli kriptosistem aileleri beş ana grupta sınıflandırılmaktadır.

4.4.1. Kafes Tabanlı Kriptografi (Lattice-based Cryptography)

Bu bölümde kuantum ataklara karşı dirençli olduğu bilinen ve kuantum sonrası kriptosistemlerin oluşturulması amacıyla çok çalışılan kafes tabanlı kriptografi ele alınmaktadır. Literatürdeki çalışmalara baktığımızda çeşitli kafes problemlerinin zorluğuna dayanan kafes tabanlı şifreleme, imzalama, anahtar değişimi ve kimlik doğrulama sistemleri oluşturulmaktadır. Kafes tabanlı kriptosistemlere ilgi duyulmasında en kötü durumda kanıtlanabilir güçlü güvenliğe sahip olmaları, verimli uygulamaları, basit yapıda olmaları ve küçük anahtar boyutuna sahip olmaları etkili olmuştur.

Kafes, n boyutlu uzayda elemanı olan n tane doğrusal bağımsız vektörün $b_1, b_2, \dots, b_n \in \mathbb{R}^n$ bütün doğrusal kombinasyonlarından oluşan bir küme olarak adlandırılmaktadır [23].

$$\mathcal{L}(b_1, b_2, \dots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}$$

$\{b_1, b_2, \dots, b_n\}$ vektörlerine kafesin bazı denilmektedir. Kafes yapıları üzerinde tanımlanmış en kısa vektör problemi (SVP), en yakın vektör problemi (CVP), küçük tamsayı çözüm problemi (SIS)

Tablo 4.4. NIST'in çağrısına gönderilen algoritmalar

	Kafes Tabanlı Kriptosistemler	Kod Tabanlı Kriptosistemler	Özet Tabanlı Kriptosistemler	Çok Değişkenli Polinomlar Tabanlı Kriptosistemler	İzojeni Tabanlı Kriptosistemler	Diğer
Anahtar Değişimi ve/veya Şifreleme	Compact LWE*					
	CRYSTALS-KYBER					
	Ding Key Exchange					
	EMBLEM and R.EMBLEM	BIG QUAKE				
	FrodoKEM	BIKE				
	Giophantus*	Classic McEliece				
	HILA5*	DAGS*				
	KCL (OKCN/AKCN/CNKE)	Edon-K*				
	KINDI	HQC				
	LAC	LAKE				Guess Again*
	Lepton*	LEDAkem*		CFPKM*		HK17*
	Lizard	LEDApkc*		DME*	SIKE	pqRSA-Encryption
	LIMA	LOCKER		SRTPI*		Ramstake
	Mersenne-756839	LOTUS				RVB*
	NewHope	McNie*				
	NTRUEncrypt	NTS-KEM				
	NTRU-HRSS-KEM	Ouroboros-R				
	NTRU Prime	QC-MDPC KEM				
	Odd Manhattan	RankSign*				
	Round2	RLCE-KEM*				
	SABER	RQC				
	Three Bears					
	Titanium					
İmzalama	CRYSTALS-DILITHIUM			DualModeMS		
	DRS*			GeMSS		
	FALCON	RaCoSS*	Gravity-SPHINCS	Gui		pqRSA-Signature
	qTESLA	pqsigRM*	SPHINCS+	HiMQ-3*		Picnic
	pqNTRUSign			LUOV		WalnutDSA*
				MQDSS		
				Rainbow		

*Kriptosistemlerin iddia edildiğinden daha az güvenli olduğunu, kırıldığını veya bu sistemlere bazı atakların gerçekleştirildiğini ifade etmektedir.
LED Acrypt algoritmasında LEDAkem ve LEDEpkc algoritmaları birleştirilmiştir.
ROLLO algoritmasında LAKE/LOCLER/Ouroboros-R algoritmaları birleştirilmiştir.
Round5 algoritmasında Hila5-Round2 algoritmaları birleştirilmiştir.

ve hatalarla öğrenme (LWE) problemi gibi birçok zor problem bulunmaktadır. Kafes tabanlı kriptosistemlerin güvenliği bu kafes problemlerinin zorluğuna dayanmaktadır.

Ajtai ve Dwork, güvenliği bir kafes probleminin en kötü durumda zorluğuna dayanan açık anahtarlı bir kriptosistem oluşturmuşlardır. Sistemin dezavantajlarından birisi büyük anahtar boyutuna sahip olmasıydı. Bunun yanı sıra, kriptoanalizler bu sistemin uygulamada yeterince güvenli olmadığını göstermişlerdir. Goldreich, Goldwasser ve Halevi tarafından CVP problemine dayanan GGH isimli bir kriptosistem önerilmiştir [23]. Hoffstein, Pipher ve Silverman tarafından NTRU isimli açık anahtarlı şifreleme sistemi önerilmiştir. Regev tarafından kafes tabanlı kriptografi için önemli bir yeri olan hatalarla öğrenme (Learning With Errors-LWE) yaklaşımı önerilmiştir [26]. Bu yaklaşım kafes problemlerinin birçoğu ile birleştirilebilmektedir. Regev, güvenliği LWE probleminin zorluğuna dayanan açık anahtarlı şifreleme şeması oluşturmuştur [26]. Bu gelişme neticesinde kafes tabanlı kriptosistemlerin kullanılabilirliği artmaya başlamıştır. Problemlerin farklı gruplar üzerinde kullanılması ile parametre boyutlarında iyileştirmelere yol açmıştır.

4.4.2. Kod Tabanlı Kriptografi (Code-based Cryptography)

Kodlama teorisi ve Goppa kodlarına dayanan kriptosistemlerdir. İlk kod tabanlı kriptosistem Robert J. McEliece tarafından önerilen açık anahtarlı şifreleme şemasıdır [23]. McEliece, açık anahtar olarak üreteç bir matris kullanırken şifreli metin hataların belli bir sayıda eklenebildiği bir kod kelimesidir [10],[23]. Elde edilen şifreli metindeki hatalar sadece gizli anahtar ile kaldırılabilmektedir. McEliece şifreleme şeması NP-zor problem olan belirti şifre çözme problemine (Syndrome Decoding Problem-SDP) dayanmaktadır. Kod tabanlı olarak şimdiye kadar kırılmayan imzalama şeması Courtois, Finiasz ve Sendrier tarafından önerilen CFS olarak isimlendirilen imzalama şemasıdır [27]. Goppa kodlarını kullanan CFS imzalama şemasında, şifresi çözülebilecek bir özet değeri elde edilene kadar tekrar tekrar özetleme işlemi yapılmaktadır [23].

Kod tabanlı kimlik doğrulama şemalarından birisi J. Stern tarafından önerilen Stern kimlik doğrulama şemasıdır [28]. Önerilen kimlik doğrulama şemasının güvenliği sendrom şifre çözme problemine dayanmakta olup sıfır bilgi paylaşımlı bir şemadır [23]. Kod tabanlı kriptosistemlerin dezavantajı, anahtar boyutunun büyük olmasından dolayı hafıza ihtiyacının fazla olmasıdır. Bu kısımda en bilinen, temel kod tabanlı sistemlere yer verilmiştir. Bunun yanı sıra, kod tabanlı şifreleme, imzalama, kimlik doğrulama ve anahtar değişimi için önerilmiş farklı kriptosistemler mevcuttur.

4.4.3. Özet Tabanlı Kriptografi (Hash-based Cryptography)

Bu alanda yapılan çalışmalara baktığımızda özet tabanlı imzalama sistemlerinin oluşturulduğunu görmekteyiz. Bu kriptosistemlerin güvenliği kullanılan özet fonksiyonlarına dayanmaktadır. Bu kısımda özet tabanlı imzalama şemalarından en yaygın bilinen Lamport-Diffie ve Merkle imzalama şemaları ifade edilecektir.

Güvenilir bir özet fonksiyonda aranan özelliklerden biri, verilen bir özet değerine karşılık gelen mesajın bulunmasının zor olmasıdır. Lamport ve Diffie özet fonksiyonların bu özelliklerinden yola çıkarak tek seferlik imzalama şeması oluşturmuştur [10]. Oluşturulan şemanın güvenliği kullanılan tek yön fonksiyona dayanmaktadır. Ancak, Lamport ve Diffie tek seferlik imzalama şemasının dezavantajı, her bir anahtar çifti ile sadece bir imzalamanın yapılabilmesi idi [28]. Merkle bu probleme çözüm önermiştir [23]. Merkle ikili özet ağaçlarını kullanarak bir açık anahtarın birden fazla doğrulama anahtarı için kullanılabilmesini sağlamıştır [23]. Oluşturulan yapıda ağacın kökü açık anahtar iken yapraklar doğrulama için kullanılacak anahtarlardır. Merkle'in imzalama şemasının güvenliği tek seferlik imzalama şemasına ve kriptografik özet fonksiyonuna dayanmaktadır. Kuantum sonrasında kullanılabilecek birçok kriptosistem önerilmiştir. XMSS kriptosistemi, matematiksel zor problemlere dayanmadan sadece kriptografik özet fonksiyonlarının özelliklerine dayanarak imzalama yapmaktadır [29]. Özet tabanlı imzalama sistemleri olarak önerilen XMSS:

Extended Hash Signatures ve Hash Based Signatures isimli kriptosistemler taslak aşamasında olan standartlardır [29], [30]. Bu standart önerileri için güvenlik analizleri yapıldığında yüksek güvenlik sağladıkları görülmektedir [29], [30].

4.4.4. İzojeni Tabanlı Kriptografi (Isogeny-based Cryptography)

Eliptik eğrilerin özellikleri ve aynı sayıda noktaya sahip iki eğri arasında izojeni oluşturmanın zorluğuna dayanan kriptosistemlerdir. Benzer yapıda oldukları için Diffie-Hellman anahtar değişim ve El-Gamal şifreleme sistemleri izojeni tabanlı kriptografi için uyarlanmıştır [31], [32]. 2011 yılında Jao ve De Feo tarafından süpersingüler izojenik Diffie Hellmann (SIDH) anahtar değişim protokolü önerilmiştir [32]. SIDH protokolü, kuantum sonrası anahtar değişim protokollerinden daha küçük anahtar boyutuna sahiptir.

4.4.5. Çok Değişkenli Polinomlar Tabanlı Kriptografi (Multivariate-based Cryptography)

Çok değişkenli polinom sistemlerine dayanan kriptosistemler, sonlu cisimlerde doğrusal olmayan çok değişkenli polinom sistemlerinin çözümünün zorluğuna dayanmaktadır. Polinom sistemlerinin tanımı ve bu kriptosistemlerin dayandıkları zor problem Bölüm 4.3'te verilmektedir.

Çok değişkenli polinom sistemlere dayanan kriptosistemlerin ilki 1988 yılında Matsumoto ve Imai tarafından yapılmıştır [33]. Yaptıkları çalışmada çok değişkenli polinomlara dayanan yeni bir asimetrik kriptosistem önermişlerdir. Bu sistemin kırılmasından sonra 1996 yılında Patarin, çok değişkenli polinomlara dayanan asimetrik kriptosistemlerin oluşturulabildiğini gösterebilmek amacıyla HFE ve IP isminde iki kriptosistem önermiştir [34]. IP sistemi sıfır bilgi paylaşımlı kimlik doğrulama ve imzalamada kullanılabilir iken HFE sistemi; şifreleme, imzalama ve kimlik doğrulama için kullanılabilen hala kırılmamış güçlü bir sistemdir [10]. Çok değişkenli polinomlar tabanlı sistemlerden biri 2005 yılında Ding ve Schmidt tarafından önerilen Rainbow imzalama şemasıdır [35]. Rainbow imzalama şemasında Yağ-Sirke (Oil-

Vinegar) imzalama şemasının genelleştirmesi yapılarak şema iyileştirilmiştir.

Çok değişkenli polinom sistemleri temelinde yapılan ilk çalışmalara bakıldığında kimlik doğrulama ve imzalama üzerine çalışıldığı görülmektedir. Haberleşen tarafların birbirlerini güvenli bir şekilde tanıyabilmeleri ve güvenilir veri paylaşımının sağlanması amacıyla kimlik doğrulama şemaları kullanılmaktadır. Bundan başka, kimlik doğrulama şemaları inkâr edememezlik ve kimlik denetimini elektronik ortamda sağlayan imzalama sistemlerinin temelini oluşturması bakımından önemlidir. Bu sebepten, çok değişkenli polinom sistemlerine dayanan kimlik doğrulama şemaları üzerinde yoğunlaşılacaktır.

2011 yılında Sakumoto vd. tarafından çok değişkenli polinomlar tabanlı sıfır bilgi paylaşımlı üç ve beş aşamalı iki kimlik doğrulama şeması önerilmiştir [36]. Önerilen şemalarda ikinci dereceden çok değişkenli polinom sistemi kullanılırken bu polinom sistemi için ikili doğrusal bir polar form oluşturulmuştur. Gizli anahtar için bir parçalama yöntemi geliştirilmiştir.

2012 yılında Sakumoto, derecesi ikiden büyük polinomlardan oluşan sistemler kullanıldığında kimlik doğrulama şemalarının nasıl oluşturulacağı üzerinde durmuştur. Üçüncü dereceden çok değişkenli polinom sistemlerine dayanan çok değişkenli polinom sistemlerine dayanan bir kimlik doğrulama şeması önermiştir [37]. Üçüncü dereceden polinom sistemlerine kimlik doğrulama şeması farklı bir polar form ve gizli anahtar parçalama metodu önermiştir. Sakumoto yaptığı çalışmada derecesi dörtten büyük olan çok değişkenli polinom sistemlerine dayanan verimli yapıların oluşturulup oluşturulamayacağı açık problem olarak bırakmıştır.

2012 yılında Nachef vd. açık probleme çözüm olabilecek bir genelleştirme önermiştir [38]. Genelleştirme d dereceden çok değişenli polinom sistemleri kullanıldığında gizli anahtarın nasıl parçalanacağını ve polar form yapısını belirtmektedir. Nachef vd. yaptıkları çalışmada genelleştirmenin kullanılabilir olduğunu göstermek amacıyla üçüncü dereceden çok değişkenli polinom sistemine dayanan kimlik doğrulama şeması önermişlerdir.

2015 yılında Monteiro vd. tarafından 2011 yılında önerilen kimlik doğrulama şeması [36] geliştirilmiştir [39]. Gizli anahtar farklı bir şekilde parçalanırken aynı polar form yapısında daha verimli bir kimlik doğrulama şeması oluşturulmuştur.

Çok değişkenli polinomlar tabanlı çalışmalar incelendiğinde kuantum sonrası için imzalama şemalarının da oluşturulduğunu görmekteyiz. 2016 yılında Chen vd. tarafından MQDSS isimli bir imzalama şeması önerilmiştir [40]. Bu şema Sakumoto vd. tarafından önerilen kimlik doğrulama şemasının imzalama şemasına dönüştürülmesiyle elde edilmiştir.

2016 yılında NIST kuantum sonrasında kullanılabilecek kriptosistemlerin oluşturulması ve standartlaşmaya gidilebilmesi amacıyla bir çağrı yayınlamıştır. 2018 yılında ilk aşaması tamamlanan bu çağrıda gönderilen kuantum sonrası güvenli kriptosistem aileleri incelendiğinde çok değişkenli polinom sistemlerine dayanan kriptosistemler dikkat çekmektedir. Bunların arasında 2016 yılında Chen vd. tarafından MQDSS isimli imzalama şemasının dayandığı kimlik doğrulama sisteminden ötürü farklılık gösterdiği görülmektedir. Çağrının ilk aşaması için çok değişkenli polinom sistemlerine dayanan kriptosistemler Tablo 4.5'te özetlenmiştir.

30 Ocak 2019'da NIST ikinci aşamaya geçen kriptosistemleri açıklamıştır. İkinci aşamaya kalan çok değişkenli polinom sistemlerine dayanan kriptosistemler Tablo 4.5'te * ile ifade edilmektedir. Kuantum sonrası güvenilir kriptosistemlerin tasarlanması ve standartlaşma süreci için bu kriptosistemlerin önemi oldukça büyüktür.

2018 yılında Soysaldı'nın tez çalışmasında sonlu cisimlerde çok değişkenli polinom sistemlerine dayanan üç tane yeni sıfır bilgi paylaşımlı kimlik doğrulama şeması önerilmiştir [41]. Önerilen kimlik doğrulama şemalarından bir tanesi Fiat-Shamir dönüşümü kullanılarak imzalama şemasına dönüştürülmüş ve güvenlik analizi yapılmıştır.

Tablo 4.5. NIST'in Kuantum Sonrası Kriptografi Projesine Gönderilen Çok Değişkenli Polinomlar Tabanlı Kriptosistemler

Açık Anahtarlı Şifreleme(PKE)/Anahtar Değişimi(KEM)	**İmzalama(Signature)**	**İmzalama(Signature) & Açık Anahtarlı Şifreleme(PKE)/Anahtar Değişimi(KEM)**
CFPKM Gioghantus	DualModeMS GeMSS* Gui HiMQ3 LUOV* MQDSS* Rainbow*	DME

* NIST'in düzenlediği çağrıya gönderilen kriptosistemlerden ikinci aşamaya kalanlar

2019 yılında Akleylek vd. çok değişkenli polinom sistemlerine dayanan kimlik doğrulama şemalarını kes-ve-seç mantığına göre sınıflandırmışlar [42]. Bulut bilişim ve IoT uygulamalarında kullanılabilirliklerini tartışmışlardır. Ayrıca, kuantum sonrası güvenilir kimlik doğrulama şemaları için standartlaşma çalışmasının gerekliliğine vurgu yapılmıştır.

2019 yılında Akleylek vd. tarafından yapılan çalışmada çok değişkenli polinomlara dayanan yeni 3 aşamalı kimlik doğrulama şeması önerilmiştir [43]. Önerilen şema daha önceki şemalar ile çeşitli kriterlere göre karşılaştırılmıştır. Bunun yanında, önerilmiş olan kimlik doğrulama şeması Fiat-Shamir dönüşümü kullanılarak imzalama şemasına dönüştürülmüştür. İmzalama şemaları için karşılaştırma tablosu verilmiştir.

2019 yılında Akleylek vd. tarafından başka bir çalışmada ise [37] nolu çalışmada Sakumoto tarafından önerilen açık probleme farklı bir bakış açısı getirilerek çözüm önerisi sunulmuştur [44]. Kimlik doğrulama şemasının nasıl oluşturulacağı ile ilgili bir taslak şema verilmiştir. Ayrıca oluşturulan çok değişkenli polinomlara

dayanan kimlik doğrulama şemalarının IoT cihazlarda kullanılabilirliğinden bahsedilmiştir.

4.5. Değerlendirmeler

Kuantum bilgisayar ile günümüzde kullanılan kriptosistemlerin güvensiz hale geleceği bilinmektedir. Bu çalışmada, var olan kriptosistemleri güvensiz hale getiren kuantum algoritmalardan bazılarına yer verilmiştir. Büyük şirketlerin geliştirdiği kuantum bilgisayarlar ve özellikleri ifade edilmiştir. Kuantum sonrası için standartlaşma sürecinin başlatılabilmesi için kuantum ataklara karşı dirençli kriptosistemlerin oluşturulması gerekmektedir. Bu kapsamda, NIST'in çağrısının önemi büyüktür. Bu nedenle, NIST'e cevap olarak gönderilen kriptosistemler ifade edilmiştir. Kuantum sonrası için NIST'in yaptığı çalışmalar anlatılmıştır. Kuantum bilgisayarlar ile problem sınıflarında oluşacak değişiklik dile getirilmiştir. Kuantum sonrası kriptografi için önerilen kriptosistem sınıfları sunularak yapılan çalışmalardan bahsedilmiştir.

Bilgi güvenliği kavramlarından olan inkâr edememezlik ve kimlik denetimi için kullanılan imzalama sistemlerinin yerine kuantum sonrasında güvenilir kriptosistemler oluşturulmalıdır. Haberleşen tarafların birbirlerini tanımalarını sağlayan kimlik doğrulama şemaları imzalama şemalarının temeli olduğundan kuantum sonrası için çok değişkenli polinom sistemleri ve kafes tabanlı kimlik doğrulama şemalarına ihtiyaç bulunmaktadır. Tasarlanan kimlik doğrulama şemaları Fiat-Shamir dönüşümü kullanılarak imzalama şemalarına dönüştürülebildiğinden kuantum sonrasında imzalama sistemleri güvenilir hale gelmiş olacaktır. Bu bakımdan, çalışmada çok değişkenli polinomlara dayanan kimlik doğrulama ve imzalama şemalarına yer verilmiştir. Kuantum sonrası güvenilir kriptosistemlerin tasarlanması hala güncel bir araştırma konusudur. NIST'in çağrısına gönderilmemiş olsa bile kuantum sonrasında güvenilir kriptosistemlerin oluşturulması kuantum sonrası süreçte alternatif sunacağından önemlidir.

Teşekkür

Bu çalışma EEEAG-116E279 proje numarası ile TÜBİTAK tarafından desteklenmiştir.

Kaynaklar

[1] J. Katz, A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone. Handbook of applied cryptography. CRC press. 1996.

[2] G. Moore. Cramming more components onto integrated circuits. Electronics Magazine Vol. 38, No. 8, pp. 1-4, 1995.

[3] R. P. Feynman. Simulating physics with computers. International journal of theoretical physics, 21(6-7), pp. 467-488, 1982.

[4] R. de Wolf. Quantum Computing: Lecture Notes. 2018.

[5] Quantum Computing Report. (2019). [Online]. Available: https://quantumcomputingreport.com/scorecards/qubit-count/. (Erişim Tarihi: 18.03.2019)

[6] C. Rugers. Risk management and the quantum threat Understanding the requirements to run Shor's algorithm to break RSA with a 2048 bit key and how to use this information to protect against the quantum threat. Leiden University. Master's Thesis. 2018.

[7] D-Wave. The D-Wave 2000QTM System. (2019). [Online]. Available: https://www.dwavesys.com/d-wave-two-system. (Erişim Tarihi: 20.01.2019)

[8] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (1997), pp. 1484-1509, 1997.

[9] L. Chen, S. Jordan, Y.K. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone. NISTIR 8105, Report on Post-Quantum Cryptography, NIST. National Institute of Standards and Technology. 2016.

[10] D. J. Bernstein, T. Lange. Post-quantum cryptography - dealing with fallout of physics success. IACR Cryptology ePrint Archieve, Report 2017/314, 2017.

[11] Stackexchange Cryptography. (2019). [Online]. Available: https://crypto.stackexchange.com/questions/35137/how-many-qubits-are-required-to-break-rsa-2048-or-4096-with-a-universal-quantum. (Erişim Tarihi: 28.01.2019)

[12] M. Mosca. Cybersecurity in an era with quantum computers: will we be ready?, QCrypt. 2015.

[13] NIST. Quantum Algorithm Zoo. (2019). [Online]. Available: https://math.nist.gov/quantum/zoo/. (Erişim Tarihi: 18.03.2019)

[14] M. Harward. Quantum computing and Shor's algorithm. 2015.

[15] M. S. Brown. Classical cryptosystems in a quantum setting. arXiv preprint quantt-ph/0404061.2004.

[16] N. D. Mermin. Quantum Computer Science: An Introduction, doi: 10.1017/CBO9780511813870. 2007.

[17] T. Moore. Quantum computing and Shor's algorithm. 2016.

[18] IBM. (2019). [Online]. Available: https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/004-Quantum-Algorithms /110-Shor'salgorithm.html. (Erişim Tarihi: 28.01.2019)

[19] L. K. Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Syposium on the Theory of Computing, pp. 212-219, 1996.

[20] M. Nielsen, I. Chuang. Quantum Computation and Quantum Information. USA: Cambridge University Press. New York, 2000.

[21] P. J. Coles et al. Quantum algorithm implementations for beginners. arXiv preprint arXiv:1804.03719. 2018.

[22] R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge University Press. 1994.

[23] D.J. Bernstein, J. Buchmann, E. Dahmen (ed.). Post-Quantum Cryptography, Springer, Berlin. 2009.

[24] Fukuoka MQ-Challenge. (2019). [Online]. Available: https://www.mqchallenge.org/. (Erişim Tarihi: 28.01.2019)

[25] NIST. Post-Quantum Cryptography. (2019). [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions. (Erişim Tarihi: 01.02.2019)

[26] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In Proc. 37th ACMSymp. on Theory of Computing (STOC), pp. 84-93, 2005.

[27] J. Buchmann, C. Coronado, M. M. Döring, D. Engelbert, C. Ludwig, R. Overbeck, A. Schmidt, U. Vollmer and Ralf-Philipp Weinmann. Post-Quantum Signatures. IACR Cryptology ePrint Archive, Report 2004/297, 2004.

[28] J. Buchmann. Post-Quantum Cryptography. 2010.

[29] A. Huelsing, D. Butin, S.-L.Gazdag, A. Mohaisen. XMSS: Extended hash-based signatures. Internet Engineering Task Force (IETF), Taslak Standart, 2016.

[30] D. McGrew, M. Curcio. Hash-based signatures. Internet Engineering Task Force (IETF), Taslak Standart, 2016.

[31] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. URL https://eprint.iacr.org/2006/145. 2006.

[32] D. Jao and L. De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In International Workshop on Post-Quantum Cryptograhy. pp. 19-34, 2011.

[33] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In EOUROCRYPT '88, Lecture Notes in Computer Science, vol 330: pp. 419-453, 1988.

[34] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In Maurer, U. M. (ed.) Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding, Lecture Notes in Computer Science, vol 1070: pp. 33-48, 1996.

[35] J. Ding, D. Schmidt. Rainbow, A new multivariate polynomial signature scheme. Lecture Notes in Computer Science, vol 3531: pp. 164-175, 2005.

[36] K. Sakumoto, T. Shirai and H. Hiwatari. Public-key identification schemes based on multivariate quadratic polynomials. In Annual Cryptology Conference, Lecture Notes in Computer Science, vol 6841: pp. 706-723, Springer, Berlin, Heidelberg. 2011.

[37] K. Sakumoto. Public-key identification schemes based on multivariate cubic polynomials. In International Workshop on Public

Key Cryptography, Lecture Notes in Computer Science, vol 7293: pp. 172-189, Springer, Berlin, Heidelberg. 2012.

[38] V. Nachef, J. Patarin and E. Volte. Zero-knowledge for multivariate polynomials. In International Conference on Cryptology and Information Security in Latin America, pp. 194-213. Springer, Berlin, Heidelberg. 2012.

[39] F. S. Monteiro, D. H. Goya and R. Terada. Improved identification protocol based on the MQ problem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E98.A no.6, pp. 1255-1265, 2015.

[40] M. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska and P. Schwabe. From 5-pass MQ-based identification to MQ-based signatures. IACR Cryptology ePrint Archive, 708, 2016.

[41] M. Soysaldı. Çok Değişkenli Polinom Sistemlerine Dayanan Kuantum Bilgisayarlar Sonrası Güvenilir Yeni Kimlik Doğrulama ve İmzalama Şemaları (Yüksek Lisans Tezi). 2018.

[42] S. Akleylek and M. Soysaldı. Identification schemes in the post-quantum area based on multivariate polynomials with applications in cloud and IoT. In Authentication Technologies for Cloud Technology, IoT and Big Data; The Institution of Engineering and Technology (The IET), pp.181-207, 2019.

[43] S. Akleylek and M. Soysaldı. A novel 3-pass identification scheme and signature scheme based on multivariate quadratic polynomials. Turkish Journal of Mathematics, 43(1), pp. 241-257, 2019.

[44] S. Akleylek, M. Soysaldı, D. E. Boubiche and H. Toral-Cruz. A novel method for polar form of any degree of multivariate polynomials with applications in IoT. Sensors, vol: *19*, 903. 2019.

Kuantum Bilgisayarlar Sonrası Güvenilir Kafes Tabanlı Kriptosistem Temelleri

BÖLÜM 5

Sedat AKLEYLEK - Kübra SEYHAN

KUANTUM BİLGİSAYARLAR SONRASI GÜVENİLİR KAFES TABANLI KRİPTOSİSTEM TEMELLERİ

Kuantum bilgisayarlar sonrası kriptografi kavramı, günümüz hesaplama sistemleri için zor olan matematiksel problemlerin çözümünde kuantum mekaniğini kullanan kuantum bilgisayarların üretilmesi ihtimali ile ortaya çıkmıştır. Kuantum bilgisayarların varlığında halihazırda kullanımda olan açık anahtarlı şifreleme sistemleri güvensiz olacaktır. Bu durum, güvenilir kriptosistemlerin varlığına ihtiyaç oluşturmuştur. Kuantum bilgisayarlar sonrası güvenilir olduğu düşünülen kafes tabanlı kriptosistemler bazı özellikleri sebebiyle birçok sistem için tercih edilir özelliktedir. Bu çalışmada kafes tabanlı kriptosistemlerin tarihsel gelişiminden bahsedilerek bu sistemleri tercih edilir kılan bazı özellikler açıklanmıştır. Ayrıca kafes tabanlı kriptosistemlerde kullanılan matematiksel tanımlara yer verilerek temel zor kafes problemleri ve bu problemler arası ilişkiler açıklanmıştır. Bunlara ek olarak, kuantum bilgisayarlar sonrası güvenilir kriptosistemlerde zor kafes problemlerinin yerinin açıklanması amacıyla NIST'in kuantum sonrası kriptografi projesinde yer alan kafes tabanlı sistemlere dair bazı özet bilgiler sunulmuştur.

5.1. Giriş

Günümüzde kullanılan açık anahtarlı kriptosistemler hesaplaması çeşitli zorluk varsayımlarına dayanan bazı matematiksel problemler temel alınarak oluşturulmuştur. Bu problemlerden tam sayı çarpanlara ayırma ve belirli gruplarda ayrık logaritma problemi, 1994 yılında Peter Shor tarafından önerilen algoritma ile

kuantum bilgisayarlar tarafından çözülebilir hale geldi. Klasik fizik kanunlarının yerini kuantum mekaniğine bırakması yaklaşımı ele alınarak oluşturulabilecek olan kuantum bilgisayarların varlığında günümüz hesaplama sistemleri tarafından kırılamayan RSA, DSA ve ECDSA gibi sistemler güvensiz hale gelecektir [1]. Bu durum kuantum bilgisayarların varlığına direnç gösterebilecek olası algoritmik problemlerin ve sistemlerin belirlenmesi gerekliliğini oluşturmuştur. Bu gereklilik sonucu kuantum sonrası güvenilir olarak değerlendirilen açık anahtarlı kriptosistemler; kod tabanlı kriptografi, özet tabanlı kriptografi, (ikinci dereceden) çok değişkenli polinom sistemleri, kafes tabanlı kriptografi, izojeni tabanlı kriptografi ve diğer sistemler başlıkları altında toplanabilir [2]. Bu sistemler, kuantum sonrası açık anahtarlı kriptosistemleri standartlaştırabilmek amacıyla yapılan proje çağrısında yer alan sistemlerdir. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST) tarafından son tarihi Kasım 2017 olarak belirlenen çağrıya 82 tane başvuru yapılmıştır. İmzalama, Şifreleme ve Anahtar Paketleme kategorilerinden oluşan başvuruların kuantum sonrası güvenilir açık anahtarlı kriptosistem sınıflarına sayısal olarak dağılımı Tablo 5.1'de özetlenmiştir [3].

Tablo 5.1. NIST Çağrısında Yer Alan Tüm Kriptosistemlerin Sınıflandırılması

	Kod Tabanlı Kriptografi	Özet Tabanlı Kriptografi	Kafes Tabanlı Kriptografi	(İkinci Dereceden) Çok Değişkenli Polinom Sistemleri	Diğer	Toplam
İmzalama	5	4	4	7	3	23
Şifreleme ve Anahtar Paketleme	19	-	24	6	10	59
Toplam	24	4	28	13	13	**82**

Tablo 5.1'de kriptosistem sınıflarına dağılımı gösterilen toplam 82 başvurudan ancak 69 tanesi tamamlanmış/uygun başvuru olarak değerlendirilmiştir. İlk aşaması 2018'de tamamlanan standartlaşma

sürecinde ikinci aşamaya geçmeye hak kazanan sistemler 30 Ocak 2019 tarihinde açıklanmıştır. Bu standartlaşma sürecinin 2023-2025 yılları arasında sonuçlanması planlanmaktadır. İlk aşamada değerlendirilen 69 sistemden 28 tanesi, ikinci aşamaya geçmeye hak kazanan 26 sistemden ise 12 tanesi kafes tabanlı kriptosistemleri içermektedir [3]. Bu sistemler kafes problemlerinin NP-zor problem sınıfına ait olması başka bir deyişle polinom zamanda çözülemeyen problemler olmaları garantisine dayanarak oluşturulmaktadır. Ayrıca günümüz hesaplama sistemlerinde çalışan algoritmalara göre performansı yüksek, zor kafes problemlerini çözmek için kuantum bilgisayarlarda polinom zamanlı çalışan bir algoritma bilinmemektedir. Tüm bu durumlar kuantum bilgisayarlar sonrası kriptografi için kafes tabanlı kriptosistemlerin güvenilir aday olarak değerlendirilmesine sebep olmuştur [1].

Kafes yapısı ilk olarak 19. yüzyılda sayılar teorisinde kullanılmaya başlamıştır. 1981 yılına gelindiğinde Lenstra tam sayı programlama üzerine yeni bir kafes indirgeme tekniği sunmuştur. Lenstra'nın önerdiği teknik bir kafesin sözde indirgenmiş bazını hesaplayan polinom zamanlı LLL (Lenstra-Lenstra-Lovasz) algoritmasının geliştirilmesine olanak sağlamıştır. Bu algoritma RSA (Rivest–Shamir–Adleman) şifreleme sistemlerine alternatif olan sırt çantası (knapsack) problemine dayalı şifreleme şemalarının kırılmasında kullanılmıştır. Bu durum açık anahtarlı şifreleme sistemlerinin kriptoanalizinde kafes indirgeme tekniklerinin kullanılmasına olanak sağlamıştır [4]. 1996 yılında ise Ajtai yapmış olduğu çalışma ile kafeslerin kriptosistemlerin oluşturulabilmesinde kullanılabileceğini göstererek kafes problemlerinin karmaşıklığını ve kriptografiyle olan ilişkisini açıklamıştır. Ajtai bu çalışmada, en kötü durum zorluğu ile bazı iyi bilinen kafes problemlerinin ortalama durum zorluğu arasındaki ilişkiyi tanımlamıştır [5]. Bir kriptosistemin güvenliği, zor kafes probleminin en kötü durum zorluğuna dayandırılmışsa göreceli olarak düşük bir ihtimalle de olsa bu sistemin kırılması ile zor kafes probleminin herhangi bir örneğinin çözülebileceği garanti edilir. Daha genel bir ifade ile kafes tabanlı kriptosistemler, en kötü durum zorluğu temel alınarak oluşturulmuşsa bu kriptosistemlerin çözülmesi göreceli olarak oldukça zordur. Bu

durum ise bazı zor kafes problemlerine dayalı birçok şifreleme sisteminin oluşturulmasına ilham vermiştir. Bu sistemlerden bazıları; en yakın vektör problemine dayalı GGH şifreleme sistemi (1997), NTRU anahtar elde etme problemine dayalı NTRU açık anahtarlı şifreleme sistemi (1998) ve hatalar ile öğrenme problemine dayalı Regev LWE tabanlı (2005) açık anahtarlı şifreleme sistemidir. Birçok kriptosisteme temel olan kafes tabanlı kriptografik yapılar [4], [6];

- En kötü durum zorluğuna dayanan güçlü güvenlik kanıtlarından yararlanması,
- Göreceli olarak verimli ve basit uygulamalar sağlaması,
- Kafes problemlerini çözmek için yüksek performanslı, polinom zamanda kuantum sonrası bilgisayarlarda çalışan algoritmaların henüz bilinememesi,
- Güvenlik ispatlarının göreceli olarak daha kolay gösterilmesi,
- Çoğunlukla vektörler ve matrisler üzerinde göreceli olarak küçük tam sayı mod değerlerinde doğrusal işlemlerden oluşması nedeniyle algoritmik açıdan sadelik ve paralellik sunması,
- İsteğe bağlı erişim politikaları ve genel amaçlı kod gizliliği için çok yönlü ve güçlü şifreleme yapıları sunması,
- Aynı güvenlik seviyesi için göreceli olarak daha küçük anahtar/imzalama boyutları sunması,

gibi faydalarından dolayı kuantum bilgisayarlar sonrası kriptografide tercih edilen sistemler arasında yer almaktadır.

5.1.1. Motivasyon

Shor algoritmasının varlığında büyük ölçekli kuantum bilgisayarların üretilebilecek olması ihtimali günümüz hesaplama sistemleri tarafından kullanılan açık anahtarlı kriptosistemleri güvensiz hale getirecektir. Bu durum kuantum bilgisayarlar sonrası güvenilir sistemlerin neler olacağı ve nasıl çalışabileceği gereksinimini ortaya çıkarmıştır. Bu gereksinim doğrultusunda bu çalışmada kuantum bilgisayarlar sonrası güvenilir olduğu düşünülen kafes tabanlı kriptosistemlerde zor kafes problemleri hakkında bilgi paylaşımını sağlamak temel amaç olarak

belirlenmiştir. Ayrıca kuantum bilgisayarlar sonrası güvenilir kriptosistemlerde zor kafes problemlerinin kullanıldığına yönelik bir bakış açısının verilmesi amacıyla NIST tarafından başlatılan standartlaşma sürecinde kafes tabanlı kriptografik yapıların yerinin ifade edilmesi hedeflenmiştir.

5.1.2. Organizasyon

Bu çalışmada Bölüm 5.1'de kuantum bilgisayarlar sonrası güvenilir sistemler belirtilerek bu sistemlerin kuantum sonrası açık anahtarlı kriptosistemlerin standartlaştırılması projesindeki yeri ifade edilmiştir. Ayrıca kafes tabanlı kriptografik yapıların tarihsel gelişimi özetlenerek sağlamış olduğu bazı özellikler belirtilmiştir. Bölüm 5.2'de kafes tabanlı kriptosistemler için temel matematiksel tanımlar ifade edilerek bu sistemlerin dayandığı bazı zor problemler özetlenmiştir. Ayrıca bu problemler arası ilişkiler detaylandırılmıştır. Bölüm 5.3'de kuantum bilgisayarlar sonrası kriptosistemlerin standartlaştırılması projesinde kafes tabanlı kriptosistemlerin yeri detaylandırılmıştır. Son bölümde ise çalışmada ele alınan temel konular özetlenmiştir.

5.2. Matematiksel Yapı

Bu bölümde kafes tabanlı kriptosistemlerin dayandığı zor problemlerin anlaşılabilmesi için gerekli olabilecek bazı matematiksel tanımlara yer verilmiştir. Ayrıca kafes tabanlı kriptosistemlerde kullanılan en kısa vektör problemi, en yakın vektör problemi, hatalar ile öğrenme problemi gibi bazı temel zor kafes problemleri ve bu problemler arası ilişkiler detaylandırılmıştır. Bu çalışmada kullanılan semboller ve anlamları Tablo 5.2'de özetlenmiştir.

Tablo 5.2. Çalışmada Kullanılan Semboller ve Anlamları

$\mathbb{R}$	: Reel sayılar.
$\mathbb{Z}$	: Tam sayılar.
$\mathfrak{R}$	: Polinomlar halkası.
p, q	**:** $p, q \in \mathbb{Z}^+$,asal sayı mod değerleri ($q > p$).
L=L(B)	**:** $\mathbb{R}^n$'de tanımlı **B** bazı vektörleri $\{b_1, \dots, b_n\}$ olan **L** tam-sıralı kafesi.

$v \in \mathbf{L}$	: v, **B** baz alınarak oluşturulmuş herhangi bir kafes vektörü.
$\|v\|$	: v vektörünün Öklit (ℓ_2) normu.
$\lambda_1(\boldsymbol{L})$	: Ardışık minimum değer.
$\lambda_n(\boldsymbol{L})$	: n tane lineer bağımsız kafes vektöründen normu en küçük kafes vektörü uzunluğu.
H(**B**)	**: B** bazı kullanılarak oluşturulan **L** kafesi için hesaplanan Hadamard oranı.
$\gamma = \gamma(n)$	: Kafes boyutuna bağlı yakınsama faktörü ($\gamma \geq 1$).
$\mathbb{Z}_q$	: $\{0, \dots, q-1\}$ ile ifade edilen $mod\ q$'da bulunan tam sayılar.
$a \epsilon \mathbb{Z}_q^{\ n}$	: Elemanları $mod\ q$'dan seçilen n boyutlu vektör.
$m \epsilon \mathbb{Z}^+$	: SIS, LWE ve türevleri için eleman sayısı.
$\lceil n \log q \rceil$	: n log q'dan büyük en küçük tam sayı.
$\beta \in \mathbb{R}^+$	: SIS ve ISIS için çözüm sınırı.
χ	: LWE probleminde $\alpha < 1$ için genişliği αq olan tam sayılar üzerinde tanımlı ayrık Gauss dağılımı.
φ	: RLWE probleminde $\alpha < 1$ için polinomlar halkası üzerinde tanımlı ayrık Gauss dağılımı.
σ	: χ ve φ ayrık Gauss dağılımları için standart sapma değeri.
$\mathbb{Z}[x]$	: Katsayıları tam sayı olan polinomlar kümesi.
$\phi(x)$	**:** $\mathbb{Z}[x]$'de tanımlı indirgenemez polinom. NTRU'da $\phi(x) = x^n - 1$ iken kafeslerde $\phi(x) = x^n + 1$ olarak seçilir.
$\Re \in \mathbb{Z}[x]/(\phi(x))$	: Katsayıları tam sayı olan polinomlar halkası, $(a_0 + a_1 x + a_2 x^2 + \cdots a_{n-1} x^{n-1}, \forall\ a_i \epsilon \mathbb{Z})$
$\Re_q \in \mathbb{Z}_q[x]/(\phi(x))$	: Katsayıları $mod\ q$'da bulunan tam sayılar olan polinomlar halkası, $(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}, \forall\ a_i \epsilon \mathbb{Z}_q)$
d	: Modül cebirsel yapısının boyutu (rankı).
$\mathbf{M} = \Re^d$	: $\forall m_i \epsilon \Re$ için $m = (m_0, \dots, m_{q-1}) \in \mathbf{M}$ ile ifade edilen d-boyutlu halka elemanlarından oluşan modül cebirsel yapısı.

5.2.1. Kafes Tabanlı Kriptografide Temel Tanımlar

Kafes tabanlı kriptosistemler Bölüm 5.1'de detaylandırılan birçok özelliği sebebiyle kuantum bilgisayarlar sonrası güvenilir sistemler arasında yer alır. Bu bölümde ise kafes tabanlı kriptosistemlerin dayandırıldığı zor kafes problemlerinin anlaşılabilmesi amacıyla bu problemlerde ele alınan kavramların matematiksel anlamları ve birbirleri ile ilişkileri açıklanmıştır. Bu bölümde açıklanan tanımlamalar [1], [6], [7], [8], [9], [10] ve [11] nolu kaynaklar referans alınarak özetlenmiştir.

Tanım 1. (Standart Kafes-Standard Lattice): $\mathbb{R}^m$'de tanımlı baz olarak adlandırılan $\{b_1, b_2, \dots, b_n\}$ lineer bağımsız vektörlerin tüm tam sayı lineer kombinasyonlarını içeren noktalar kümesidir.

$$\boldsymbol{L} = \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n : a_i \in \mathbb{Z},\ \mathrm{i} = (1, .. n)\}$$

Kafesi oluşturabilmek için lineer bağımsız vektörler topluluğu (baz) kullanımına ihtiyaç duyulmaktadır.

Tanım 2. (Baz): $\{b_1, \dots, b_n\} \in \mathbb{R}^m$'de tanımlı lineer bağımsız vektörler olsun. $\mathbf{B} = [b_1, \dots, b_n] \in \mathbb{R}^{mxn}$ matrisi tarafından üretilen kafes matematiksel olarak;

$$\boldsymbol{L}(\boldsymbol{B}) = \{Ba\ \in \mathbb{Z}^{\,n}\} = \sum_i^n a_i b_i \colon\ a_i\ \in \mathbb{Z}$$

ile ifade edilebilir. **L**(**B**) kafesi, **B** matrisinin sütun vektörlerinin tüm tam sayı lineer kombinasyonlarını içerir. **L** kafesi oluşturan lineer bağımsız vektör kümesine ise baz denir.

Dikkat edilmelidir ki; Tanım 1 ile açıklanan standart kafes tanımında **L** kafesini oluşturan n tane baz vektörünün her biri $\mathbb{R}^m$'de tanımlıdır. Ancak kafes tabanlı kriptosistemlerde standart kafeslerin özelleşmiş hali olan tam-sıralı kafesler kullanılmaktadır.

Tanım 3. (Tam-sıralı Kafes-Full-rank Lattice): **L** kafesini tanımlayan n tane $b_i \in \mathbb{R}^m$ baz vektörlerini içeren $\mathbf{B} \in \mathbb{R}^{mxn}$ matrisi kare matris iken (m = n), det(**L**(**B**)) = |det(**B**)| şartı

sağlanıyorsa **L**(**B**) kafesi tam-sıralı kafes olarak adlandırılır ($\forall\, b_i \in \mathbb{R}^n$).

Baz vektörlerine bağlı olarak tanımlanan kafeslerde her bir nokta bir vektöre karşılık geleceği için ilk olarak bu vektörlerin sayısal anlamda ölçülebilirliği ifade edilmelidir. Geometrik ortamda bir vektörün uzunluğu genellikle norm kavramı ile ilişkilendirilmektedir.

Tanım 4. (Uzunluk-Norm): Reel sayılarda tanımlı $v \in \mathbb{R}^n$ vektörü için Öklit normu ve sonsuz norm değerleri ;

$$\text{Öklit Norm } (\ell_2)\text{: } \|v\| = \sqrt{|v_0|^2 + \cdots + |v_{n-1}|^2}$$

$$\text{Sonsuz Norm } (\ell_\infty)\text{: } \|v\|_\infty = max|v_i|$$

eşitlikleri ile hesaplanır. Standart kafeslerde kullanılan cebirsel yapının (vektörler) değiştirilmesi ile Tanım 12 ve Tanım 13 ile açıklanan farklı kafes kullanımları oluşturulmaktadır. Örneğin, vektörler ile polinomlar halkasının eşyapı (izomorf) olmaları özelliğinden yararlanılarak ideal kafesler oluşturulmuştur. İdeal kafeslerde her bir vektör bir polinoma karşılık gelmektedir. Bu durum ise polinomlar halkası üzerinde tanımlı k=$k_0 + k_1 x + k_2\, x^2 + \cdots + k_{n-1} x^{n-1} \epsilon\, \Re$, $\forall\, k_i \in \mathbb{R}$ polinomu için Öklit normu ve sonsuz norm değerlerinin hesaplanabilmesini gerektirmektedir.

$$(\ell_2)\text{: } \|k\| = \sqrt{\|k_0\|_\infty^2 + \cdots + \|k_{n-1}\|_\infty^2}$$

$$(\ell_\infty)\text{: } \|k\|_\infty = \max\{\|k_i\|_\infty\},\ \|k_i\| = \sqrt{\|k_0\|_\infty^2 + \cdots + \|k_{n-1}\|_\infty^2}$$

Tanım 4'te açıklanan ℓ_2 ve ℓ_∞ norm kavramları Bölüm 5.2.2'de detaylandırılacak zor kafes problemlerinin zorluk derecelerinin ifade edilmesinde kullanılan bir hesaplama aracı olarak düşünülmektedir.

Vektörler arasındaki açıya göre farklı bazlar oluşturulabilmektedir. Örneğin, iki vektörün birbirine dik olması (ortogonal) durumunda oluşturulan bazlar ile dik olamamaları ile oluşturulan bazlar iki farklı yapı olarak kafes tabanlı

kriptosistemlerde kullanılmaktadır. Bu anlamda bazların sınıflandırılmasında kullanılan kavramların anlaşılabilmesi için ilk önce geometrik anlamda ortogonallik kavramını açıklanmalıdır.

Tanım 5. (Ortogonal Vektör): **L** kafesini tanımlayan $\mathbf{B} = \{b_1, \dots, b_n\} \in \mathbb{R}^{nxn}$ bazı vektörleri için $\forall\, i \neq j: b_i \cdot b_j = 0$ ise bazı tanımlayan vektörler ortogonal olarak ifade edilir.

Ortogonallik kavramı zor kafes problemlerinin çözülebilme sınırlarını etkileyen faktörlerden biri olarak değerlendirilmektedir. Vektörlerin ortogonallik özelliğini sağlayıp sağlamadığının ölçülebilirliği ise Hadamard oranı ile belirlenmektedir.

Tanım 6. (Hadamard Oranı): Verilen bir kafesi oluşturan baz vektörlerinin ortogonalliği hakkında çıkarım yapılabilmesine olanak sağlayan Hadamard oranı;

$$H(\mathbf{B}) = \left(\frac{\det(\mathbf{L})}{\|b_1\| \cdot \|b_2\| \cdots \|b_n\|}\right)^{\frac{1}{n}}$$

eşitliği ile hesaplanmaktadır. Ayrıca, **L** kafesi ile kafesi üreten baz **B** arasındaki ilişki Hermite-Hadamard eşitsizliği;

$$\det(\mathbf{L}) = |\det(\mathbf{B})| \leq \|b_1\| \cdot \|b_2\| \cdots \|b_n\|$$

ile ilişkilendirildiğinde bu eşitsizlikten elde edilen;

$$0 < H(\mathbf{B}) \leq 1$$

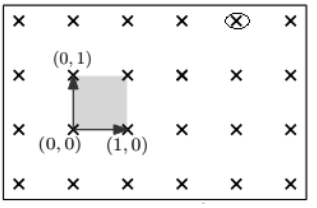
aralık ele alınarak Hadamard oranının ($H(\mathbf{B})$) 1'e yakın olması, bazda bulunan vektörlerin ortogonal olmasının bir ölçüsü olarak ifade edilmektedir.

Vektörler arasındaki açının değişmesine bağlı olarak farklı özellikte bazlar oluşturulabilmektedir. Bu durum ise bir kafesi tanımlayan birden fazla baz vektörü kümesinin olabilmesine imkan sağlamaktadır. Bu kapsamda kafesi tanımlayan baz vektörü kümeleri özelliklerine göre iki ana başlık altında toplanır.

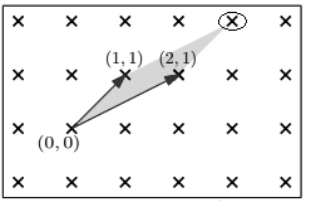
Tanım 7. (İyi Baz, Kötü Baz): Tanım 6'da açıklanan Hadamard oranı göreceli olarak 1'e yakın olan başka bir deyişle ortogonal olan normu küçük baz vektörleri **L** kafesini oluşturuyorsa iyi baz

olarak adlandırılırken Hadamard oranı 0'a yakın olan, ortogonal olmayan baz vektörleri ise kötü baz olarak adlandırılır.

Şekil 5. 1. İki Boyutlu Uzayda İyi Baz [12]



Şekil 5. 2. İki Boyutlu Uzayda Kötü Baz [12]



İki boyutlu uzayda iyi baz özelliklerini sağlayan baz vektörleri Şekil 5.1'de ve kötü baz özelliklerini sağlayan baz vektörleri Şekil 5.2'de örneklendirilmiştir.

Şekil 5.1'de $b_1 = \begin{bmatrix}1\\0\end{bmatrix}$, $b_2 = \begin{bmatrix}0\\1\end{bmatrix}$ baz vektörleri için $a_1 = 3 \quad a_2 = 2$ iken $v = \begin{bmatrix}2\\3\end{bmatrix} \in \mathbf{L}$ kafes noktası elde edilirken,

Şekil 5.2'de $g_1 = \begin{bmatrix}2\\1\end{bmatrix}$, $g_2 = \begin{bmatrix}1\\1\end{bmatrix}$ baz vektörleri için $a_1 = 1 \quad a_2 = 1$ iken $v = \begin{bmatrix}2\\3\end{bmatrix} \in \mathbf{L}$ aynı kafes noktası elde edilir.

b_1, b_2 ve g_1, g_2 baz vektörlerinin tüm tam sayı lineer kombinasyonları ile aynı kafes noktaları oluşturulabilmektedir. Bu durum ise aynı kafesi oluşturan birden fazla baz vektörü kümesinin olabileceği yaklaşımını destekler bir örnek olarak değerlendirilmelidir. Bu yaklaşım bazı kafes tabanlı kriptosistemlerin oluşturulmasına sebep olmuştur. Örneğin, 1997 yılında önerilen GGH şifreleme sisteminde [11] şifre çözme aşamasında geri dönüşün yapılabilmesi kafesi oluşturan baz vektörlerinin iyi-kötü baz özelliklerini sağlama durumları ile ilişkilendirilmiştir.

Kafesi oluşturan birden fazla baz vektörü kümesinin (matrisinin) olabilmesini etkileyen bir diğer yapı ise Unimodular matris kavramıdır. Çünkü **L** kafesini oluşturan herhangi bir baz matrisi verildiğinde, Unimodular matris ile kafesi oluşturabilecek yeni baz

matrisleri üretilebilmektedir. Başka bir deyişle, **L** kafesini oluşturan iki farklı A ve B baz matrisleri arasında $A = BU$ eşitliğini sağlayan U, Unimodular matrisi vardır.

Tanım 8. (Unimodular Matris): Bütün satır ve sütun vektörleri lineer bağımsız olan, tersi alınabilir kare matris özelliklerine sahip, tekil olmayan matrislerdir. U unimodular matrisinin determinantı ya 1 ya da -1 olmalıdır.

$$\det(U) = \pm 1$$

Kafes tabanlı kriptosistemlerde Unimodular matrisin özelliklerinden yararlanılarak sistemde kullanılan açık anahtar-gizli anahtar ikilileri elde edilebilmektedir. Örneğin, GGH şifreleme sisteminde iyi baz vektörleri gizli anahtar olarak belirlenir. İyi baz vektörleri ile Unimodular matris özelliğini sağlayan rastgele bir matris kullanılarak elde edilen kötü baz vektörleri ise açık anahtar olarak bu sistemde kullanılmaktadır.

Tüm kafes vektörlerinin geometrik anlamda ifade edilebilmesi bu vektörlerin normlarının değerlendirilmesi ile sağlanmaktadır. Örneğin, ℓ_2 norm ele alındığında kafes vektörlerinin tanımlı olduğu cebirsel yapıda belirli özellikleri sağlayan en küçük norma sahip olan vektörün bulunması zor olarak nitelendirilen bir kavramdır. Bu kavram ise ardışık minimum değer ile ifade edilebilir.

Tanım 9. (Ardışık Minimum Değer-Successive Minima): Normu 0'dan farklı en kısa kafes vektörünün uzunluğu ($\lambda_1(\mathbf{L})$) olarak tanımlanmaktadır. **L** kafesinde bulunan $\{v_1,\ldots,v_n\}$ vektörleri ele alındığında bu vektörlerin ardışık en küçüğü matematiksel olarak;

$$\begin{aligned}\lambda_1(\boldsymbol{L}) &= \min\{\|v_i - v_j\| : v_i \neq v_j \in \boldsymbol{L}\} \\ &= \min\{\|v_i\| : v_i \in \boldsymbol{L}, v_i \neq 0\}\end{aligned}$$

eşitliği ile ifade edilebilir. Ayrıca, **L** kafesinde bulunan n tane lineer bağımsız vektör $\{v_1,\ldots,v_n\}$ için n. ardışık minimum değer ($\lambda_n(\boldsymbol{L})$);

$\lambda_1 = \|v_1\|$: **L** kafesinde bulunan en kısa vektör uzunluğu,

$\lambda_2 = \|v_2\|$: **L** kafesinde v_1 haricinde bulunan vektörler için en kısa vektör uzunluğu,

$\lambda_3 = \|v_3\|$: **L** kafesinde v_1 ve v_2 haricinde bulunan vektörler için en kısa vektör uzunluğu,

$\vdots$

$\lambda_n = \|v_n\|$: **L** kafesinde $v_1,\ldots,v_{n-1}$ haricinde bulunan vektörler için en kısa vektör uzunluğu,

eşitliği ile hesaplanmaktadır.

Ardışık minimum değer kavramı, Bölüm 5.2.2'de detaylandırılacak olan kafesler ile ilgili bazı zor problemlerin tanımlanmasında belirli bir yakınsama faktörüne kadar problemlerin çözüm sınırlarının ifade edilmesinde kullanılmaktadır.

Bölüm 5.2.2'de açıklanacak olan NTRU anahtar elde etme probleminin zorluğuna dayandırılarak polinomlar halkasını ($\Re$) kullanan ilk kriptografik yapı oluşturulmuştur [10]. Bu problemin anlaşılabilmesi ve kafesler ile olan ilişkisinin değerlendirilebilmesi için çevrimsel çarpma işlemi ve üçlü polinom kavramları tanımlanmalıdır.

Tanım 10. (Çevrimsel Çarpma İşlemi-Convolutional Product-$*$): $n \geq 1$ asal sayı iken ebob(n,q)=1 olarak seçildiği durumda $\Re$ ile ifade edilen polinomlar halkasından seçilen;

$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} \epsilon \Re$ ve $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1}x^{n-1} \epsilon \Re$ polinomlarının çevrimsel çarpımı;

$$a(x) * b(x) = c(x),$$

$$c(x) = \sum_{k=0}^{n-1} \left(\sum_{i+j \equiv k \ (mod\ n)} a_i b_j \right) x^k$$

eşitliği ile hesaplanır ve temelde $(x^n - 1)$ halkasına göre modüler indirgeme işlemi gerçekleştirilir. Çevrimsel çarpma işleminin yapıldığı bir örnek şu şekildedir:

Örnek 5.1. $x^5 - 1$ halkasında $a(x) = 1 - 2x + 4x^3 - x^4$ ve $b(x) = 3 + 4x - 2x^2 + 5x^3 + 2x^4$ polinomları çarpılırsa;

$a(x) * b(x) = 3 - 2x - 10x^2 + 21x^3 + 5x^4 - 16x^5 + 22x^6 + 3x^7 - 2x^8$ eşitliğinde x^5 yerine 1 yazılarak indirgeme yapılır.

$$= 3 - 2x - 10x^2 + 21x^3 + 5x^4 - 16 + 22x + 3x^2 - 2x^3$$

$$= -13 + 20x - 7x^2 + 19x^3 + 5x^4 \, \epsilon \, \Re = \mathbb{Z}\,[x]/(x^5 - 1)$$

Eğer $\Re \in \mathbb{Z}\,[x]/(x^5 - 1)$ yerine $\Re_{11} \in \mathbb{Z}_{11}\,[x]/(x^5 - 1)$ halkasında işlemler gerçekleştirilseydi katsayılar $mod\ 11$'e indirgenerek

$$a(x) * b(x) = 9 + 9x + 4x^2 + 8x^3 + 5x^4 \ \epsilon \, \Re_{11}$$

sonucu elde edilecektir.

NTRU tabanlı sistemlerde kullanılan Bölüm 5.2.2'de özetlenen NTRU anahtar elde etme probleminin kullanıldığı NTRU şifreleme siteminde gizli anahtar değerleri üçlü polinomlardan seçilirken polinomlar halkası üzerinde çalışıldığı için çevrimsel çarpma işlemi kullanılarak indirgeme işlemleri gerçekleştirilir. Bu problemin NTRU tabanlı sistemlerde kullanımı için üçlü polinom kavramını tanımlanmalıdır.

Tanım 11. (Üçlü Polinomlar-Ternary Polynomials): $a(x) \, \epsilon \, \Re$ polinomu katsayılarının $mod\ q$ ya da $mod\ p$'de indirgenmesi ile a(x) polinomu $\Re_q$ ya da $\Re_p$'nin elemanı olarak değerlendirilir. n≥1 asal sayı iken p ve q'nun $\text{ebob}(n, q) = \text{ebob}(n, p) = 1$ eşitliklerini sağlayacak şekilde seçildiği durumda $h_1, h_2 \in \mathbb{Z}^+$ tanımlı ise a(x) için;

$$T(h_1, h_2) = \begin{cases} a(x) \text{ polinomunun katsayılarından } h_1 \text{ tanesi } 1'\text{dir.} \\ a(x) \text{ polinomunun katsayılarından } h_2 \text{ tanesi } -1'\text{dir.} \\ a(x) \text{ polinomunda kalan katsayılar } 0'\text{dir.} \end{cases}$$

eşitliği ile tanımlanan $T(h_1, h_2)$ polinomları üçlü polinomlar olarak adlandırılır. Başka bir deyişle, tüm katsayıları $\{-1,0,1\}$ olan polinomlar olarak ifade edilir.

Kafes tabanlı kriptosistemlerde temel olarak Tanım 1 ile ifade edilen standart kafesler kullanılırken sistemlerin güvenliklerinin dayandırıldığı zor problemlerde kullanılan cebirsel yapının değişmesine bağlı olarak kullanılan kafesin özellikleri de değişmektedir.

Tanım 12. (İdeal Kafes): $f(x) = x^n + f_n x^{n-1} + \cdots + f_1 \epsilon \mathbb{Z}$ [x] iken katsayıları $mod\ q$'da tam sayılar olan bütün polinomları içeren $\Re_q \in \mathbb{Z}_q$[x]/(f(x)) halkası üzerinde tanımlanan kafeslere denir. f(x) derecesi n olan indirgenemez monik (öncü katsayısı 1 olan) bir polinom ise $\Re_q \in \mathbb{Z}_q$[x]/(f(x)) halkası derecesi (n-1)'den küçük polinomları içerir. Örneğin, $n = 2^k$ iken $\Re_q \in \mathbb{Z}_q$[x]/$(x^n + 1)$ halkası ideal bir kafes iken $(x^n - 1)$'in indirgenebilir bir polinom olması nedeniyle $\Re_q \in \mathbb{Z}_q$[x]/$(x^n - 1)$ halkası ideal bir kafes oluşturmaz.

Tanım 13. (Modül Kafes): Modül kafesleri hem standart kafesleri hem de ideal kafesleri genelleştiren yapı olarak ifade edilir. Derecesi n'den küçük katsayıları tam sayı olan polinomlar halkası üzerinde sonlu olarak üretilen modüllere karşılık gelen d boyutlu $\Re_q$ halkasında $\boldsymbol{M} = \Re_q^d = \mathbb{Z}_q^d[x]/(x^n + 1)$ ile tanımlanan kafeslere denir.

Bu bölümde kafes tabanlı zor problemlerin anlaşılabilmesi için kavramsal olarak ele alınan tanımlara ait genel bir özet sunulmuştur.

5.2.2. Kafeslerde Zor Problemler

Kafes tabanlı kriptosistemler aynı güvenlik seviyesi için göreceli olarak daha küçük anahtar/imzalama boyutları sunarken bu sistemlerin güvenliği zor kafes problemlerinin polinom zamanda çözülememesi ile garanti edilir [1]. Bu bölümde içerebilecekleri kavramlar Bölüm 5.2.1'de özetlenen kafes tabanlı kriptosistemlerin dayandığı NP-tam ve NP-zor problem sınıflarında ifade edilen

polinom zamanda çözülemeyen bazı zor kafes problemleri ve bu problemler arası ilişkiler yorumlanmıştır. Bu bölümde açıklanan zor problemler [5], [6], [7], [8], [9], [13], [14], [15] nolu kaynaklar referans alınarak özetlenmiştir.

Kafes tabanlı kriptosistemler güvenlik garantisi olarak zor kafes problemlerini temel almaktadır. Bu sistemlerde kullanılan temel ve güncel bazı zor kafes problemleri şu şekilde özetlenebilir:

Tanım 14. (En Kısa Vektör Problemi-Shortest Vector Problem-SVP): **L** kafesinde normu 0'dan farklı olan en kısa kafes vektörü v'yi bulma problemidir.

$$SVP\colon \|v\| = \lambda_1(\boldsymbol{L})$$

SVP'de **L** kafesinde bulunan belirli şartları sağlayan tek bir kafes vektörü aranmaktadır. Ancak v kafes vektörü ele alındığında $\pm v$ vektörlerinin normları eşit olacağı için tek bir en kısa kafes vektörü yoktur. Bu yaklaşımla belirli bir yakınsama faktörüne kadar en kısa vektörünün (SVP_γ) hangisi olacağı sorusuna cevap aranmıştır.

Tanım 15. (Yaklaşık En Kısa Vektör Problemi-Approximate Shortest Vector Problem-SVP_γ): **L** kafesinde bulunan normu 0'dan farklı en kısa kafes vektörünün en fazla γ katı kadar uzunluğa sahip olabilecek kafes vektörünü bulma problemidir.

$$\text{SVP}_\gamma\colon \|v\| \leq \lambda_1(\boldsymbol{L})$$

SVP_γ probleminin ℓ_∞ normda NP-zor olduğu 1981 yılında Emde Boas tarafından kanıtlanırken ℓ_2 normda NP-zorluğu ise 1998 yılında Ajtai tarafından kanıtlanmıştır [16]. Kafes problemlerinin zorlukları yakınsama faktörü değeri ile ilişkilendirilmiştir. Yakınsama faktörü (γ) ise kafes boyutunun bir fonksiyonudur. Bu ilişki sonucu kafes boyutu arttıkça hesaplaması zor olan problemler daha da zorlaşır. Bu kapsamda Tablo 5.3'de SVP_γ probleminin ℓ_2 ve ℓ_∞ normda hangi yakınsama faktörü değerlerinde NP-zor olduğu gösterilmiştir.

Kafeslerle ilgili her bir zor problem arama ve karar verme problemleri şeklinde tanımlanabilmektedir. SVP_γ probleminde en

kısa vektör aranırken, bu problemin karar verme problemi şeklinde tanımlanması ise GapSVP_γ problemi ile ifade edilmektedir.

Tanım 16. (Yaklaşık Olarak En Kısa Vektöre Karar Verme Problemi-Decisional Approximate Shortest Vector Problem-GapSVP_γ): **L** kafesinde bulunan normu 0'dan farklı en kısa kafes vektörünün uzunluğunun bulunduğu aralığa karar verme problemidir.

$$\text{GapSVP}_\gamma : \lambda_1(\boldsymbol{L}) < 1 \;||\; \lambda_1(\boldsymbol{L}) \geq \gamma$$

SVP_γ probleminde belirli şartı sağlayan tek bir en kısa kafes vektörü aranmaktadır. Belirli şartları sağlayan birden fazla en kısa vektörün olması durumu ise SIVP_γ problemi ile ifade edilir.

Tanım 17. (Yaklaşık En Kısa Bağımsız Vektörler Problemi-Approximate Shortest Independent Vector Problem-SIVP_γ): **L** kafesinde bulunan normu en küçük kafes vektörünün en fazla γ katı kadar uzunluğa sahip olan n tane kafes vektörünü bulma problemidir.

$$\text{SIVP}_\gamma : \|v_i\| \leq \gamma \lambda_n(\boldsymbol{L}), \qquad S = \{v_i\} \subset \boldsymbol{L}$$

SVP problemi ve türevlerinde değerlendirilen vektörler sahip oldukları norm değerleri ve tanımlı olduğu kafeste bulunan diğer vektörlerin norm değerlerinin kıyaslanması yaklaşımını ele alır. Böyle bir durum kafes vektörü olmayan bir nokta verildiğinde bu problemlerin nasıl değişeceğinin gösterilmesi gerekliliğini oluşturmaktadır. Bu gereklilik sonucu kafes vektörü olan bir nokta ile kafes vektörü olmayan bir noktanın değerlendirildiği problemlere ihtiyacı oluşturmuştur.

Tanım 18. (En Yakın Vektör Problemi-Closest Vector Problem-CVP): Kafes noktası olmayan $t \in \mathbb{R}^n$ noktası verildiğinde, bu noktaya en yakın olan kafes vektörü $v \in \boldsymbol{L}$'yi bulma problemidir.

$$\text{CVP}: min\|t - v\| = \min\{\|t - v\| \mid v \in \boldsymbol{L}\}$$

CVP problemi, Tanım 14 ile açıklanan SVP probleminin homojen olamayan çözümü olarak değerlendirilebilir. Başka bir deyişle, SVP'de orjine yakın kafes noktası aranırken CVP'de ise kafes noktası olmayan hedef noktasına yakın kafes noktası aranır. Ayrıca CVP problemi birçok kafes tabanlı kriptosistemin oluşturulmasına kaynaklık etmiştir. Örneğin, CVP probleminin zorluğuna dayanarak oluşturulan GGH şifreleme sistemi. SVP problemine benzer şekilde belirli bir yakınsama faktörüne kadar CVP probleminin çözümü ise CVP_γ ile ifade edilebilir.

Tanım 19. (Yaklaşık En Yakın Vektör Problemi-Approximate Closest Vector Problem-CVP_γ): Kafes noktası olmayan $t \in \mathbb{R}^n$ noktası verildiğinde, bu noktaya en fazla γ kadar yakın olan kafes vektörü $v \in \boldsymbol{L}$'yi bulma problemidir.

$$\mathrm{CVP}_\gamma : min\|t - v\| < \gamma \min\{\|t - v\| \mid v \in \boldsymbol{L}\}$$

CVP_γ probleminin ℓ_2 ve ℓ_∞ normda NP-zor olduğu 1981 yılında Emde Boas tarafından kanıtlanmıştır [16]. Bu zorluk garantisi, CVP_γ problemini kafes tabanlı kriptosistemler için tercih edilir kılmıştır. [16] nolu çalışmadan uyarlanan Tablo 5.3'de SVP_γ ve CVP_γ problemlerinin farklı norm kavramlarının değerlendirildiği durumda hangi yakınsama faktörü değerleri için NP-zor olduğu özetlenmiştir. Örneğin, SVP_γ probleminin ℓ_2 normda NP-zor olabilmesi için yakınsama faktörü $\boldsymbol{2^{log^{1-\varepsilon} n}}$ olarak seçilmelidir.

Tablo 5.3. SVP_γ ve CVP_γ Problemlerinin ℓ_2 ve ℓ_∞ normlar için NP-zor Durum Tablosu

	ℓ_2		ℓ_∞	
Problemler	SVP_γ	CVP_γ	SVP_γ	CVP_γ
NP-Zor	$\boldsymbol{2^{log^{1-\varepsilon} n}}$	$\boldsymbol{2^{log^{1-\varepsilon} n}}$	$\boldsymbol{n^{\frac{1}{log\ log\ n}}}$	$\boldsymbol{n^{\frac{1}{log\ log\ n}}}$
NP-Zor Olmama Durumu	$\boldsymbol{\sqrt{\frac{n}{log\ n}}}$	$\boldsymbol{\sqrt{\frac{n}{log\ n}}}$	$\boldsymbol{\frac{n}{log\ n}}$	$\boldsymbol{\frac{n}{log\ n}}$

Çalışmanın bu bölüme kadar kafes tabanlı kriptosistemler için temel zor problemler ve bu zor problemler arası ilişkiler özetlenmiştir. Temelinde bu problemler yer alan kafes tabanlı bazı önemli fonksiyonlar ve zor problemler çalışmanın kalan kısmında özetlenecektir.

Güncel kafes tabanlı kriptosistemlerde neredeyse bütün protokollerin temel aldığı iki tane ortalama durum zorluğuna dayanan problem vardır. Bunlar SIS ve LWE problemleridir. SIS problemi belirli özellikleri sağlayan kafeslerde en kısa vektörü bulma problemi olarak değerlendirilmektedir.

Tanım 20. (Kısa Tam Sayı Çözüm Problemi-Short Integer Solution Problem-SIS): 1996 yılında Ajtai tarafından tanımlanmıştır. Belirli büyüklükte sonlu bir toplamsal grubun rastgele elemanları verildiğinde, bu elemanların toplamlarını 0 yapan yeterince kısa tam sayı kombinasyonunu bulma problemi olarak ifade edilmektedir.

SIS: m tane düzgün rastgele $a_i \in \mathbb{Z}_q^n$ vektörlerini sütun vektörü olarak kabul eden $A \in \mathbb{Z}_q^{nxm}$ matrisi verilsin. $\|z\| \leq \beta < q$ şartını sağlayan, 0'dan farklı tam sayı vektör $z \in \mathbb{Z}^m$'yi bulma problemidir.

$$f_A(z) = Az = \sum_{i=1}^{m} a_i z_i = 0 \ \in \mathbb{Z}_q^n$$

SIS probleminin temelini oluşturan parametrelerin seçimi ile ilgili dikkat edilmesi gereken bazı temel durumlar vardır.

1. n, problem için ana zorluk parametresidir. q ve β değerlerinin n'nin birer polinomu olduğu durumlarda göreceli olarak n>100 olarak seçilir [6].
2. SIS probleminin zorluk garantisi için q ve β parametreleri arasındaki ilişki β < q olarak belirlenmelidir. Aksi takdirde i. pozisyonunda q değerini içeren $z = (0, \dots, q, \dots) \in \mathbb{Z}^m$ vektörü SIS problemi için uygun bir çözüm olacaktır.
3. SIS'in çözümü olarak değerlendirilen z vektörünün normu için belirlenen $\|z\| \leq \beta$ sınırın ortadan kaldırılması

durumunda SIS problemi Gauss indirgeme ile polinom zamanda çözülebilecektir.

4. SIS probleminin en az bir tane çözümünün var olabilmesini garanti etmek için $\bar{m} = \lceil n\, loq\, q \rceil$ iken $m \geq \bar{m}$ ve $\beta \geq \sqrt{\bar{m}}$ seçilmelidir.

SIS probleminin zorluğu en kötü durum zorluğuna dayanan problemler ile ifade edilmiştir. Belirli parametre koşulları dikkate alındığında ortalama durum zorluğuna dayanan SIS probleminin zorluğu, en kötü durum zorluğuna dayanan GapSVP_γ ve SIVP_γ problemleri ile ifade edilir.

Teorem 1. SIS Probleminin Zorluğu: $m = poly(n)$, $\beta > 0$ ve $q \geq \beta poly(n)$ iken GapSVP_γ ve SIVP_γ problemleri için keyfi n boyutlu kafeslerde en-kötü durumda yakınsama faktörü $\gamma = \beta poly(n)$ olsun. Parametrelerin seçimindeki sınırlamalar göz önüne alındığında SIS problemini çözmek en az GapSVP_γ ve SIVP_γ problemlerini çözmek kadar zordur [6].

SIS problemi temel geometri kavramları ile ilişkilendirildiğinde homojen lineer denklem sistemlerini hatırlatmaktadır. Bu problemde A matrisi lineer denklem sistemlerindeki katsayılara karşılık gelirken z vektörü ise bilinmeyenler olarak değerlendirilebilir. Bu durumda lineer denklem sistemlerinde olduğu gibi SIS probleminde de homojenliği sağlayan sonucun 0'a eşit olması durumu araştırılır. Bu durum haricinde kalan durumların değerlendirildiği homojen olmayan lineer denklem sistemleri ise ISIS problemine karşılık gelmektedir.

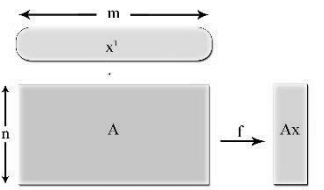
Tanım 21. (Homojen Olmayan Kısa Tam Sayı Çözüm Problemi-Inhomogeneous Short Integer Solution Problem-ISIS): Belirli büyüklükte sonlu bir toplamsal grubun rastgele elemanları ele alındığında, elemanların toplamlarını u gibi bir tam sayı yapacak olan yeterince kısa tam sayı kombinasyonu $z \in \mathbb{Z}^m$'yi bulma problemidir.

$$f_A(z) = Az = \sum_{i=1}^{m} a_i z_i = u \in \mathbb{Z}_q^n$$

Ajtai, SVP gibi en kötü durumda çözümü zor olan bir problemin varlığında ortalama durum zorluğuna dayanan tek-yönlü bir fonksiyonun (Ajtai fonksiyonu) var olduğunu kanıtlamıştır [5]. Ajtai'nin teoremine dayanarak, eğer polinom zamanda bir A algoritması SIS problemini çözerse, polinom zamandaki herhangi bir boyut kafesinde SVP problemini çözebilecek etkin bir B algoritması vardır çıkarımı elde edilebilir.

Tanım 22. (Ajtai Fonksiyonu): 1996 yılında Ajtai tarafından tanımlanan fonksiyon ilk önerilen yapılardan birdir. Temelde sonlu bir uzayda matris vektör çarpımı işlemi yapılır. Çakışmaya karşı dirençli olma özelliğinden dolayı birçok kriptosistemde özet (hash) fonksiyonların tanımlanmasına kaynaklık etmiştir. Şekil 5.3'de Ajtai fonksiyonu işlemleri görsel olarak ifade edilirken, Algoritma 1 ile parametre seçimlerine bağlı olarak fonksiyonun işleyişi özetlenmiştir.

Şekil 5. 3. Ajtai Fonksiyonu



Algoritma 1 Ajtai Fonksiyonu

Girdi: $n, m \in \mathbb{Z}$ ve $q > 2$ asal, $A \in \mathbb{Z}_q^{nxm}$, $x \in \{0,1\}^m$.

Çıktı:

$$f : \{0,1\}^m \rightarrow \mathbb{Z}_q^n$$
$$x \rightarrow Ax \bmod q$$

Ajtai Fonksiyonunun Özellikleri:

- Teorem 1 ile ifade edilen SIS probleminin zorluğu göz önüne alındığında Ajtai fonksiyonunda $x, y \in \{0,1\}^m$

girdileri için bir çakışma olsun. SIS problemi için çözüm vektörü olan z vektörü bu çakışma göz önüne alındığında $z = x - y$ ile ifade edilebilir. Bu durumu SIS probleminin zorluğu ile ilişkilendirilirse çakışmaların bulunduğu,

$$F_A = \left\{ f_A^* \colon \{0,1\}^m \to \mathbb{Z}_q^n, A \in \mathbb{Z}_q^{nxm} \right\}$$

F_A fonksiyon ailesinin bulunabilmesi en az GapSVP_γ ve SIVP_γ problemlerinin çözümü kadar zordur. Bu zorluk Ajtai fonksiyonun çakışmaya karşı dirençli özet fonksiyonu olarak ifade edilebilmesine olanak sağlamıştır.

- Ajtai, bu fonksiyonların tersine çevrilmesinin ortalama durumda zor olduğunu kanıtlamıştır. Bu durum ise Ajtai fonksiyonlarının tek-yönlü ve çakışmaya karşı dirençli özet fonksiyonları olarak değerlendirilmesine sebep olmuştur [5].
- Ajtai fonksiyonunda parametrelerin seçiminde $m > n \log q$ şartı sağlanırsa bu fonksiyonun girdi değerini sıkıştırdığı gözlemlenir. Dolayısıyla, m değerinin seçilmesinde sıkıştırma seviyesi ve çakışmanın olmaması varsayımı noktasında bir denge olmalıdır.
- $A \in \mathbb{Z}_q^{nxm}$ ile hesaplanan $\mathcal{O}(mn)$ anahtar boyutu değeri diğer anahtar boyutu değerleri ile karşılaştırıldığında verimsiz olması nedeniyle Ajtai fonksiyonu pratik uygulamalarda tercih edilmemektedir.

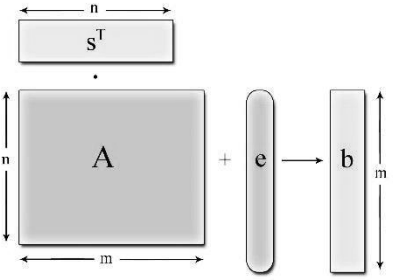
Ajtai fonksiyonu ile başlayan SIS problemi ve türevleri ile devam eden süreçte bu tanımlara belirli hata değerlerinin eklemesi durumunda problemin nasıl değerlendirileceği sorusuyla birçok kafes tabanlı sisteme temel olan LWE problemi tanımlanmıştır.

Tanım 23. (Hatalar ile Öğrenme Problemi-Learning With Errors Problem-LWE): 2005 yılında Oded Regev tarafından ortalama durum zorluğuna dayanan bir problem olarak tanımlanmıştır. Gizli değer $s \in \mathbb{Z}_q^n$ vektörü için $a_i \in \mathbb{Z}_q^{n'}$de düzgün rastgele değerler iken e_i hata teriminin χ dağılımından seçildiği durumda LWE dağılımı;

$$(a_i, b_i = < s, a_i > + e_i \ mod\ q) \in \mathbb{Z}_q^n x \mathbb{Z}_q$$

ile ifade edilebilir. $a_i \in \mathbb{Z}_q^n$'de düzgün rastgele değerlerin sütun vektörü olarak kabul edildiği $A \in \mathbb{Z}_q^{nxm}$ matrisine bağlı olarak LWE probleminin parametreleri ve işlevi Şekil 5.4 ile özetlenmiştir.

Şekil 5. 4. LWE Problemi



Örnek 5.2. LWE dağılımından örnek üretebilmek için açık kaynak kodlu matematik yazılımı olan SageMath kullanılabilmektedir [17]. LWE dağılımına ait parametreler rastgele olarak n=4 (boyut), m=3 (örnek sayısı), q=17 (mod değeri) ve σ=3 (hata dağılım parametresi) seçildiğinde LWE dağılımına ait örneklerin üretilebilmesi için kullanılan SageMath fonksiyonları ve açıklamaları şu şekilde özetlenebilir.

SageMath Fonksiyon ve Parametreleri:

- ✓ *from sage.crypto.lwe import LWE:* Dağılım çeşidi olarak LWE belirlenir.
- ✓ *from sage.stats.distributions.discrete_gaussian_integer import DiscreteGaussianDistributionIntegerSampler*: LWE dağılımında kullanılan hata terimlerinin seçildiği dağılım olarak tam sayılar üzerinde tanımlı ayrık Gauss dağılımı belirlenir.
- ✓ *D = DiscreteGaussianDistributionIntegerSampler(3.0):* Ayrık Gauss dağılımı parametresi σ=3 olarak belirlenir.
- ✓ *lwe = LWE(n=4, q=17, D=D);* n=4, q=17 ve σ=3 parametreli LWE dağılımı oluşturulur.
- ✓ *L = [lwe() for _ in range(3)]:* m=3 ile LWE dağılımından rastgele 3 örnek belirlenir.

Yukarıda örneklenen SageMath fonksiyonları ile üretilen LWE dağılımından rastgele seçilen $(a_i, \boldsymbol{b_i})$ ile ifade edilen 3 farklı örnek şu şekildedir:

$$((3, 5, 11, 6), \mathbf{13})$$

$$((14, 5, 0, 14), \mathbf{16})$$

$$((11, 16, 4, 5), \mathbf{0})$$

Üretilen örnekler incelendiğinde her bir değer mod 17'de bulunan tam sayılardan oluşurken her bir örnek için parametrelerin $\mathbb{Z}_{17}^{4} x \mathbb{Z}_{17}$'de tanımlı olduğu görülmektedir. İlk örnek için $a_1 = (3, 5, 11, 6)$ iken seçilen gizli s değerine bağlı olarak üretilen $\boldsymbol{b_1} = \mathbf{13}$'dür.

LWE problemi; arama ve karar verme problemleri olarak iki kısımdan oluşur.

Arama LWE: LWE dağılımından seçilen m tane bağımsız örnek verildiğinde bu örneklerden gizli değer $s \in \mathbb{Z}_q^n$ vektörünü bulma problemidir.

$$\begin{aligned} a_1 &\leftarrow \mathbb{Z}_q^n, \quad & b_1 &= < s, a_1 > + e_1 \ mod\ q \\ a_2 &\leftarrow \mathbb{Z}_q^n, \quad & b_2 &= < s, a_2 > + e_2 \ mod\ q \\ & & \vdots & \\ a_m &\leftarrow \mathbb{Z}_q^n, \quad & b_m &= < s, a_m > + e_m \ mod\ q \end{aligned}$$

Karar Verme LWE: m tane bağımsız örnek (a_i, b_i) verildiğinde bu örneklerin LWE dağılımına mı yoksa normal dağılıma mı ait olduğuna karar verme problemidir. Başka bir deyişle, LWE örnekleri ile normal dağılım örnekleri arasında ayrım yapma problemidir.

$$(a_i, b_i) = \begin{cases} (a_i, b_i = < s, a_i > + e_i \ mod\ q), & \text{LWE örneği} \\ Diğer\ (a_i, b_i), & \text{Rastgele örnek} \end{cases}$$

Not 5.1. SIS probleminden LWE problemine geçişte başka bir terimin eklenmesi durumunda problemin nasıl değiştiğinin gözlenmesi amaçlanmıştır. Bu anlamda e_i hata terimlerinin χ

dağılımından seçildiği durumda arama ve karar verme LWE problemleri ortalama durum zorluğa sahip bir problemken e_i hata teriminin olmadığı durumda arama ve karar verme LWE problemleri Gauss indirgeme ile etkin bir şekilde çözülebilir. Bu yüzden parametrelerin seçildiği dağılım ve parametreler arası ilişkiler doğru bir şekilde değerlendirilmelidir.

LWE probleminin zorluğu en kötü durum zorluğuna dayanan problemler ile ifade edilmiştir. Belirli parametre koşulları dikkate alındığında ortalama durum zorluğuna dayanan LWE probleminin zorluğu, en kötü durum zorluğuna dayanan GapSVP_γ ve SIVP_γ problemleri ile ifade edilir.

Teorem 2. LWE Probleminin Zorluğu: $m = poly(n),\ q \leq 2^{poly(n)}$, $0 < \alpha < 1,\ \alpha q \geq 2\sqrt{n}$ parametreli ayrık Gauss hata dağılımı χ iken GapSVP_γ ve SIVP_γ problemleri için keyfi n boyutlu kafeslerde yakınsama faktörü olarak $\gamma = \mathcal{O}(\frac{n}{\alpha})$ seçilsin. Tüm bu parametre seçimleri dikkate alındığında karar verme LWE probleminin çözülmesi en az GapSVP_γ ve SIVP_γ problemlerinin kuantum olarak çözümü kadar zordur.

Kafeslerle ilgili zor problemlerden SIS ve LWE için kullanılan cebirsel yapının değiştirilmesi ile anahtar boyutu daha küçük, daha hızlı ve verimli sistemlerin elde edilmesi amaçlanmıştır. Bu problemlerde vektörler ile polinomlar halkasının eşyapı özelliği dikkate alınarak ve parametrelerinin seçildiği cebirsel yapı polinomlar halkası olarak belirlenerek problemlerin halka cebirsel yapısı ile kullanımları tanımlanmıştır.

Tanım 24. (Halka SIS Problemi-Ring SIS Problem-RSIS): 2002 yılında Micciancio tarafından önerilen RSIS probleminde; m tane rastgele $a_i \in \mathfrak{R}_q$ elemanlarını içeren $a \in \mathfrak{R}_q^m$ vektörü tanımlansın. Bu vektörün normu için $\|z\| \leq \beta$ şartını sağlayacak en az bir tane $z_i \neq 0$ elemanı içeren (normu 0'dan farklı), kısa $z \in \mathfrak{R}^m$ vektörünü bulma problemidir.

$$f_a(z) =< a, z >= a^T \cdot z = \sum_i (a_i \cdot z_i) = 0 \ \in \mathfrak{R}_q$$

SIS-RSIS ilişkisi:

- ✓ RSIS'in çözümü olan her halka elemanı $z_j \in \Re$, SIS'in çözümü olan n tane $z \in \mathbb{Z}^m$ tam sayı değerine karşılık gelir.
- ✓ SIS ile kıyaslandığında RSIS'in temel avantajları göreceli olarak sıkılığı ve verimliliğidir.
- ✓ Yeterince kısa çözümün varlığını garanti edebilmek için SIS probleminde örnek sayısı ve boyut arasındaki ilişki $m \approx n \log q$ iken RSIS'de $m \approx \log q$ olarak ifade edilir.

Tanım 25. (Halka LWE Problemi-Ring LWE Problem-RLWE): 2010 yılında Lyubashevsky, Peikert ve Regev tarafından halka tabanlı hatalar ile öğrenme problemi tanımlanmıştır. $s \in \Re_q$ gizli değeri için $a \in \Re_q$ düzgün rastgele iken e hata teriminin φ hata dağılımından seçildiği durumda $\Re_q$ x $\Re_q$'da tanımlı RLWE dağılımı;

$$(a, b = s \cdot a + e \; mod \; q) \in \Re_q x \Re_q$$

eşitliği ile ifade edilebilir.

Karar Verme RLWE: m tane birbirinden bağımsız $(a_i, b_i) \in \Re_q x \Re_q$ örneğin RLWE dağılımına mı yoksa düzgün dağılıma mı ait olduğuna karar verme problemidir.

Örnek 5.3. RLWE problemi için Örnek 5.2'de seçilen parametreler ile RLWE dağılımından örnekler üretilebilmesi için Örnek 5.2'de açıklanan SageMath fonksiyonlarından hata dağılımı ve örneklerin üretildiği dağılım fonksiyonu değiştirilerek RLWE örnekleri üretilebilir. Elde edilen RLWE dağılımından rastgele seçilen $(a_i, \boldsymbol{b_i})$ ile ifade edilen 3 farklı örnek şu şekildedir:

((7, 0, 12, 10), **(0, 14, 8, 7)**)

((16, 4, 15, 3), **(3, 14, 14, 14)**)

((3, 14, 3, 5), $(\mathbf{2}, \mathbf{13}, \mathbf{2}, \mathbf{0})$)

Üretilen örnekler incelendiğinde her bir değer mod 17'de bulunan tam sayılardan oluşurken her bir örnek için parametrelerin $\mathfrak{R}_{17}x\mathfrak{R}_{17}$'de tanımlı olduğu görülmektedir. İlk örnek için $a_1 = (7, 0, 12, 10)$ iken seçilen gizli s değerine bağlı olarak üretilen $\boldsymbol{b_1} = (\mathbf{0}, \mathbf{14}, \mathbf{8}, \mathbf{7})$'dir.

RLWE probleminin zorluğu LWE probleminde olduğu gibi en kötü durum zorluğuna dayanan problemler ile ifade edilmiştir. Belirli parametre koşulları dikkate alındığında RLWE probleminin zorluğu, en kötü durum zorluğuna dayanan SVP_γ problemi zorluğu ile ifade edilir.

Teorem 3. RLWE Probleminin Zorluğu: $m = poly(n)$, derecesi n olan tam sayı katsayılı polinomlar halkası $\mathfrak{R}$, uygun $mod\ q$ değeri ve hata oranı ($\alpha < 1$) için φ hata dağılımı verilsin. Bazı $\gamma = poly(n)/\alpha$ değerleri için $\mathfrak{R}$'de tanımlı keyfi ideal kafesler göz önüne alındığında; RLWE problemi en az SVP_γ probleminin kuantum olarak çözümü kadar zordur [14].

LWE-RLWE ilişkisi:

- ✓ LWE ile kıyaslandığında RLWE'nin temel avantajları göreceli olarak sıklığı ve verimliliğidir.
- ✓ Polinomlar halkasında Fourier dönüşümü ile çarpma işlemi $\mathcal{O}(nlogn)$'e indirgenir. Bu yüzden RLWE'de n tane sözde rastgele değer $\mathcal{O}(1)$ zamanda üretilebilir.
- ✓ RLWE'de her bir örnek (a_i, b_i), n boyutlu sözde rastgele halka elemanı $b_i \in \mathfrak{R}_q$ oluştururken, LWE'de bir tane sözde rastgele $b_i \in \mathbb{Z}_q$ değerini oluşturulur.

LWE ve RLWE problemleri ele alındığında güvenlik ve maliyet arasında bir denge sağlaması amacıyla MLWE problemi önerilmiştir.

Tanım 26. (Modül LWE Problemi-Module LWE Problem-MLWE): 2013 yılında Brakerski ve arkadaşları modül tabanlı hatalar ile öğrenme problemini tanımlamıştır. n boyutlu $\mathfrak{R}$ halkasında $M = \mathfrak{R}^d$ modülü tanımlansın. s $\in \mathfrak{R}_q^d$ gizli değeri için

a $\in \mathfrak{R}_q^d$ düzgün rastgele seçilen bir değer iken e hata teriminin φ hata dağılımından seçildiği durumda MLWE dağılımı;

$$(a, b = s \cdot a + e \; mod \; q) \in \; \mathfrak{R}_q^d x \mathfrak{R}_q$$

eşitliği ile ifade edilebilir.

Karar Verme MLWE: m tane birbirinden bağımsız $(a_i, b_i) \in \mathfrak{R}_q^d x \mathfrak{R}_q$ örneğin MLWE dağılımına mı yoksa düzgün dağılıma mı ait olduğuna karar verme problemidir.

Örnek 5.4. MLWE problemi için Örnek 5.2'de seçilen parametreler ile MLWE dağılımından örnekler üretilebilmesi için Örnek 5.2'de açıklanan SageMath fonksiyonları ile MLWE dağılımı üretebilmek için henüz fonksiyon oluşturulmamıştır. Problemler arası ilişkilerin açıklanabilmesi için Örnek 5.3 ele alınarak Modül boyutu $d = 3$ seçildiğinde üretilebilecek MLWE dağılımından rastgele seçilen $(a_i, \boldsymbol{b_i})$ ile ifade edilen 3 farklı örnek şu şekilde olabilir:

(((7, 0, 12, 10), (0, 14, 8, 7), (4, 6, 7, 1)), **(2, 1, 6, 9)**)

(((6, 4, 1, 3), (3, 12, 0, 11), (2, 4, 6, 8)), **(4, 11, 3, 7)**)

(((13, 14, 3, 7), (1, 4, 7, 9) ,(2, 3, 2, 0)), **(2,12,10,4)**)

Üretilen örnekler incelendiğinde her bir değer mod 17'de bulunan tam sayılardan oluşurken her bir örnek için parametrelerin $\mathfrak{R}_{17}^3 x \mathfrak{R}_{17}$'de tanımlı olduğu görülmektedir. İlk örnek için $a_1 = ((7, 0, 12, 10), (0, 14, 8, 7), (4, 6, 7, 1))$ iken seçilen gizli s değerine bağlı olarak üretilen $\boldsymbol{b_1} = (\mathbf{2}, \mathbf{1}, \mathbf{6}, \mathbf{9})$'dur.

Standart LWE probleminin tanımlanması ile başlayan süreç ve buna bağlı olarak farklı cebirsel yapıların sağlayacağı faydalar düşünülerek oluşturulan LWE problemi kullanımları Tanım 25 ve Tanım 26'da açıklanmıştır. Bu açıklamaların tümü ele alındığında çeşitli parametrelere göre problem özelliklerinin nasıl değiştiği Tablo 5.4'de özetlenmiştir. Örneğin, LWE problemi için asimptotik

anlamda ihtiyaç duyulan eleman sayısı $\mathcal{O}(n^2)$ iken RLWE için $\mathcal{O}(n)$ ve MLWE için ise $\mathcal{O}(nd)$'dir.

Tablo 5.4. Farklı Cebirsel Yapılar İçeren LWE Tabanlı Problemlerin Karşılaştırılması

LWE Tabanlı Problemler	*Cebirsel Yapı*	*Hata Dağılımı*	*Eleman Sayısı*	*Kafes Zorluğu*
LWE	$\mathbb{Z}_q^n \times \mathbb{Z}_q$	χ	$O(n^2)$	standart SIVP
RLWE	$\Re_q \times \Re_q$	φ	$O(n)$	ideal SIVP
MLWE	$\Re_q^d \times \Re_q$	φ	$O(nd)$	modül SIVP

LWE problemine dayalı sözde rastgele sayı üreteçlerinin verimliliğini artırmak amacıyla LWR problemini tanımlanmıştır.

Tanım 27. (Yuvarlamalar ile Öğrenme Problemi-Learning With Roundings Problem-LWR): 2012 yılında Banerjee ve arkadaşları yuvarlamalar ile öğrenme problemini tanımlamıştır. Bu problemde LWE probleminden farklı olarak hatalar belirleyici role sahiptir. Gizli bilginin saklanması için LWR probleminde hatalar eklenmez bunun yerine bir p katsayısı ile yuvarlama işlemi yapılır ve rastgele olmayan hata değeri $\mathbb{Z}_q$'dan $\mathbb{Z}_p$'ye düşürülerek oluşturulur. Gizli değer $s \in \mathbb{Z}_q$ vektörü için $a \in \mathbb{Z}_q^n$'de düzgün rastgele değerler iken LWR dağılımı;

$$(a, b = \lfloor p/q\ (< s, a > mod\ q) \rceil\ ) \in \mathbb{Z}_q^n x \mathbb{Z}_p$$

eşitliği ile ifade edilebilir.

Karar Verme LWR: m tane birbirinden bağımsız $(a, b) \in \mathbb{Z}_q^n x \mathbb{Z}_p$ örneğin LWR dağılımına mı yoksa düzgün dağılıma mı ait olduğuna karar verme problemidir.

LWE-RLWE ilişkisi düşünülerek LWR probleminde kullanılan cebirsel yapının değiştirilmesi ile RLWR problemi oluşturulmuştur.

Tanım 28. (Halka Tabanlı Yuvarlamalar ile Öğrenme Problemi-Ring Learning With Roundings Problem-RLWR): Gizli değer $s \in$

$\Re_q$ vektörü için $a \in \Re_q$ 'da düzgün rastgele değerler iken RLWR dağılımı;

$$(a, b = \lfloor\ p/q\ (s \cdot a\ \ mod\ q)\rceil) \in \Re_q x \Re_p$$

eşitliği ile ifade edilebilir.

Karar Verme RLWR: m tane birbirinden bağımsız $(a, b) \in \Re_q x \Re_p$ örneğin RLWR dağılımına mı yoksa düzgün dağılıma mı ait olduğuna karar verme problemidir.

Not 5.2. Banerjee ve arkadaşları yeterince büyük mod değerleri için RLWR probleminin en az RLWE problemi kadar zor olduğunu kanıtlamıştır [15].

Hatırlanacağı üzere Bölüm 5.2.1'de NTRU tabanlı şifreleme sistemlerinde kullanılan Tanım 10 ile çevrimsel çarpma işlemi ve Tanım 11 ile üçlü polinomların matematiksel anlamı ifade edilmişti. Bu kavramlar ele alındığında NTRU tabanlı sistemlere temel oluşturan NTRU anahtar elde etme problemi şu şekilde tanımlanabilir:

Tanım 29. (NTRU Anahtar Elde Etme Problemi-NTRU Key Recovery Problem): $h(x) \in \Re_q$ polinomu verildiğinde $h(x)$ ile aralarında $f(x) * h(x) = g(x)\ \ mod\ q$ ilişkisi bulunan göreceli olarak çok küçük katsayılara sahip $f(x)$ ve $g(x)$ polinomlarını bulma problemidir.

Not 5.3. NTRU anahtar elde etme probleminin;

- Kaba kuvvet (brute-force) gibi yaklaşımlarla pratik olarak çözülememesi,
- Belirli kafes sınıflarında hem ℓ_2 norm hem de ℓ_∞ normda polinom zamanda çözülemeyen bir problem (NP-zor) olan SVP problemini çözmeye eş değer olması,

bu problemin zor bir matematik problem olarak değerlendirilmesine neden olmaktadır.

NTRU anahtar elde etme problemi zorluğu temel alınarak 1998 yılında Hoffstein, Pipher ve Silverman tarafından açık anahtarlı NTRU şifreleme sistemi oluşturulmuştur [10]. $\Re = \mathbb{Z}[x]/(x^n - 1)$ ile ifade edilebilen çevrimsel (rankı n olan) polinomlar halkası kullanılarak tanımlanmıştır. Bu sistem pratik olarak verimlidir ve oldukça sıkı anahtarlara sahiptir. NTRU şifreleme sisteminde özel anahtarın bulunması ve dolayısıyla sistemin çözülmesi, NTRU anahtar elde etme probleminin çözülmesi ile sağlanmaktadır. NTRU şifreleme sisteminde kullanılan parametreler;

- ✓ $h \in \mathbb{Z}^+$ ve $q > (6h + 1)p$.
- ✓ $f(x) \in T(h + 1, h)$ ve $g(x) \in T(h, h)$ Tanım 11 ile ifade edilen özellikleri sağlayan üçlü polinomlar.
- ✓ $F_q(x)$: $\Re_q$'da $f(x)^{-1}$.
- ✓ Açık anahtar: $h(x) = F_q(x) * g(x) \in \Re_q$.

iken gizli anahtarın bulunması ile NTRU şifreleme sisteminin kırılabilmesi ancak NTRU anahtar elde etme probleminin çözülmesi ile sağlanacaktır.

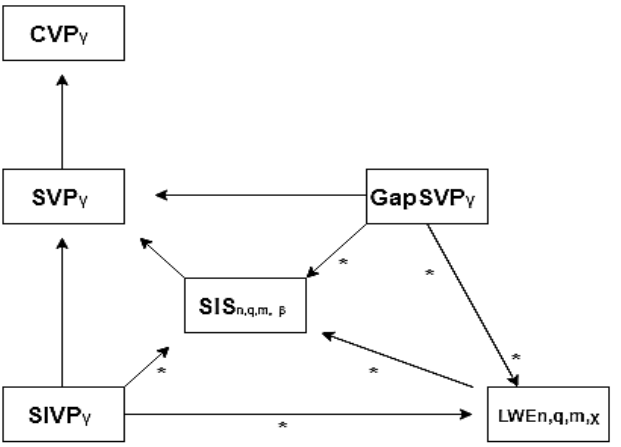
Bu bölümde kafes tabanlı bazı zor problemler detaylandırılmıştır. Bu zor problemler kafes tabanlı kriptosistemlerin güvenliklerinin garantisi olarak değerlendirilmektedir. Bu bağlamda bu problemler arası olası geçişler ve indirgemeler sistemlerin anlaşılması açısından önemli olarak değerlendirilmektedir.

5.2.3. Kafes Tabanlı Kriptosistemlerde Kullanılan Temel Zor Problemler Arası İlişkiler

Kafes tabanlı kriptosistemlerde bulunan zor bir problemde her örnek zor olmak zorunda değildir. Belirli bir alt sınıf problemin çözülmesinin kolay olduğu ortaya çıkarsa, bu zor problemin alt sınıf problemine dayanan bir şifreleme sistemi güvenli olmayacaktır. Kısaca sistemlerin güvenliği zor problemlerin güvenlik garantileri ve içerdikleri alt sınıf zor problemler ile ilişkilidir [18].

Kafes tabanlı kriptosistemlerde zor problemlerin zorlukları bu problemler arasındaki indirgemeler ile ifade edilmektedir. Problem Y'nin bütün örneklerini çözebilen herhangi bir yöntem Problem X'in örneklerini çözmek için kullanılabiliyorsa Problem X, Problem Y'ye indirgenebilir denir. Bu durumda Problem Y, Problem X'den daha kolay olmayacaktır. Başka bir deyişle, Problem Y en az Problem X kadar zor olacaktır. [9] nolu çalışmadan uyarlanan Şekil 5.5'te bazı kafes problemleri arasındaki indirgemeler gösterilerek zor kafes problemleri arasındaki ilişki ifade edilmiştir.

Şekil 5. 5. Temel Zor Kafes Problemleri Arası İlişkiler



Örnek olarak; SVP_γ ve CVP_γ arasındaki ilişki ele alınırsa SVP_γ problemi polinom zamanda CVP_γ problemine indirgenebilir. Başka bir deyişle, CVP_γ'nın hesaplama karmaşıklığı en az SVP_γ'nın hesaplama karmaşıklığı kadardır. Ayrıca SVP_γ problemi, CVP_γ problemini çözmede kullanılabilmektedir. Bu ilişki CVP_γ probleminin zorluğunu temel alarak oluşturulmuş bir sistemin varlığında SVP_γ probleminin bu sistemin kırılmasında kullanılabileceği anlamına gelmektedir.

LWE ve $GapSVP_\gamma - SIVP_\gamma$ problemleri arasındaki ilişki Teorem 2 ile ifade edilen durumdur. Başka bir deyişle, LWE probleminin zorluğu çeşitli parametre koşullarının sağlandığı durumlar (Şekil

5.5'de *) ele alındığında kuantum olarak en az GapSVP_γ ve SIVP_γ problemleri kadar zordur. Bu yaklaşım Şekil 5.5'de GapSVP_γ ve SIVP_γ problemlerinden LWE problemine çizilen ok ile ifade edilmiştir.

Bölüm 5.2'de kafes tabanlı kriptosistemlerde kullanılan temel tanımlar, bazı zor kafes problemleri ve bu kafes problemleri arası ilişkiler hakkında özet bilgiler sunulmuştur.

5.3. Kuantum Sonrası Kriptografi İçin Standartlaşma Projesi

Uygulama alanında kafes tabanlı kriptosistemlerin ne anlama geldiğini açıklayabilmek için bu bölümde NIST'in kuantum bilgisayarlar sonrası açık anahtarlı kriptosistemleri standartlaştırma projesinde kafes tabanlı kriptosistemlerden bazıları için başvuruların yapıldığı sistem kategorisine bağlı olarak ait oldukları kafes türleri, parametre kümeleri ve dayandıkları zor problem türlerine dair özet bilgiler verilmiştir.

Günümüz hesaplama sistemleri için zor olan matematiksel problemlerin çözülebilmesi amacıyla kuantum mekaniğini temel alan kuantum bilgisayarların üretilmesi veya üretilebilecek olması ihtimali hâlihazırda kullanımda olan açık anahtarlı şifreleme sistemlerini güvensiz hale getirecektir. Bu durum veri iletişiminde korunan gizlilik ve bütünlük kavramlarını tehlikeye sokacaktır. Hem kuantum bilgisayarlar hem de günümüz hesaplama sistemlerine karşı güvenli, mevcut iletişim protokolleri ile birlikte çalışabilecek sistemlerin elde edilebilmesi amacıyla 2016 yılı sonlarında NIST bir çağrıda bulundu [19]. Bu çağrıda katılımcılar bir veya daha fazla güvenlik kategorisinde farklı parametre kümeleriyle sistemlerini sunmaya davet edildi. Başvurularda katılımcılardan güvenlik taleplerini destekleyen Kriptoanalizi sağlamaları istenmiştir. Ayrıca bu Kriptoanalizin her bir parametre kümesi için güvenlik parametresinin boyutunun tahmin edilmesinde kullanılması istenmiştir. Hatırlanılacağı üzere NIST'in çağrısı ile ilgili Bölüm 5.1'de yapılan başvurular ve kategorileri hakkında özet bilgiler sunulmuştu. Tablo 5.1'de açıklanan toplam

82 tane başvurudan 69 tanesinin ilk aşama için kabul edildiği ifade edilirken bu sayının ikinci aşamada 26'ya düştüğü açıklanmıştır. İlk aşamada değerlendirilen 69 başvuru incelendiğinde 23 tanesinin güvenliği Bölüm 5.2.2'de detaylandırılan LWE ve NTRU tabanlı problem ailelerine dayanmaktadır [20].

NIST'in yapmış olduğu çağrıya ilk aşama sonucu gönderilen bazı kafes tabanlı kriptosistemler incelendiğinde, sistemlerin dayandıkları zor problemlere bağlı olarak kullanılan kafes türlerinin değiştiği gözlemlenmiştir. NIST'in kuantum bilgisayarlar sonrası standartlaşma projesinde ilk aşamada yer alan kafes tabanlı kriptosistemlerin sınıflandırılması sonuçları [21] nolu çalışmadan uyarlanan Tablo 5.5 ile özetlenmiştir.

Tablo 5.5. NIST'e Gönderilen Kafes Tabanlı Sistemlerin Sınıflandırılması

NIST Sistemler	Zor Problem	Şema Türü			Kafes Türü
		Açık Anahtarlı Şifreleme	*İmzalama*	*Anahtar Paketleme*	
Emblem	LWE	✓	X	✓	Standart Kafes
Lizard	LWE/LWR	✓	X	✓	
uRound2.PKE	LWR/RLWR	✓	X	✓	
LOTUS	LWE	✓	X	✓	
NTRUEncrypt	NTRU	✓	X	X	
FrodoKEM	LWE	✓	X	✓	
qTESLA	RLWE	X	✓	X	İdeal Kafes
FALCON	NTRU	X	✓	X	
Ding Key Exchange	RLWE	X	X	✓	
REmblem	RLWE	✓	X	✓	
NTRU-HRSS-KEM	NTRU	X	X	✓	
Lima	RLWE	X	X	✓	
NTRU Prime	NTRU	✓	X	X	
Hila5	RLWE	✓	X	✓	
SABER	MLWR	✓	X	✓	Modül Kafes
pqNTRUSign	NTRU	X	✓	X	
CRYSTALS-KYBER	MLWE	✓	X	✓	
CRYSTALS-DILITHIUM	MLWE/MSIS	X	✓	X	
KINDI	MLWE/MSIS	✓	X	✓	

Örneğin, Tablo 5.5'de özellikleri ifade edilen *Lizard* sistemi açık anahtarlı şifreleme ve anahtar paketleme kategorisinde yer alırken tam sayılar üzerinde tanımlı Tanım 1'de açıklanan standart kafes yapısına bağlı olarak oluşturulan zorluğu LWE/LWR problemlerine dayandırılan bir sistemdir. Başka bir örnek olarak *qTESLA* sistemi ise imzalama kategorisinde yer alırken polinomlar üzerinde tanımlı halka cebirsel yapısını temel alan Tanım 12'de

açıklanan ideal kafes yapısına bağlı olarak oluşturulan RLWE tabanlı bir sistem olduğu söylenebilir.

Kafes tabanlı kriptosistemler temel aldıkları zor problemlerde kullanılan parametrelerin seçimine göre sistemin güvenliği şekillenmektedir. Bu kapsamda NIST'in kuantum bilgisayarlar sonrası standartlaşma projesinde ilk aşamada yer alan kafes tabanlı kriptosistemlerin parametre kümeleri, dayandıkları zor problem türü ve güvenlik kategorilerine dair sonuçlar [20] nolu çalışmadan uyarlanan Tablo 5.6 ile özetlenmiştir.

Tablo 5.6'de n; problem boyutunu, q; problemde kullanılan mod değerini, σ; problemin türüne göre değişen hata dağılımın standart sapma değerini, gizli dağılım; problemde kullanılan rastgele elemanların seçildiği dağılımı, ϕ; problemin tanımlandığı $\mathbb{Z}_q[x]/(\phi)$ polinomlar halkası için indirgenemez polinomu ve güvenlik seviyesi ise kuantum Kriptoanalize karşı AES ve güvenilir SHA ailesine göre sistemlerin sağladığı güvenlik seviyelerini göstermektedir. Örnek olarak, Ding Key Exchange sisteminin dayandığı zor problem halkalar üzerinde tanımlı hatalar ile öğrenme problemi (RLWE) iken AES 128-bitlik güvenlik garantisinin sağlanabilmesi için $n = 512,\ q = 120883$ olarak seçilmiştir. Ayrıca hata dağılımı normal dağılımdan seçilerek bu dağılımın standart sapma değeri $\sigma = 4.19$ olarak hesaplanmıştır.

İlk aşamada 69 başvurunun değerlendirildiği standartlaştırma sürecinin ikinci aşaması 30 Ocak 2019 tarihinde açıklanmıştır. NIST tarafından yapılan açıklamaya göre ikinci aşamaya geçmeye hak kazanan kriptosistemlerin İmzalama, Şifreleme ve Anahtar Paketleme kategorilerine göre dağılımı şu şekildedir:

- **Şifreleme ve Anahtar Paketleme Sistemleri:**
  BIKE, Classic McEliece, CRYSTALS-KYBER, FrodoKEM, HQC, LAC, LEDAcrypt (LEDAkem/LEDApkc birleşimi), NewHope, NTRU (NTRUEncrypt/NTRU-HRSS-KEM birleşimi), NTRU Prime, NTS-KEM, ROLLO (LAKE/LOCKER/Ouroboros-R birleşimi), Round5 (Hila5/Round2 birleşimi), RQC, SABER, SIKE, Three Bears.

- **İmzalama Sistemleri:**
  CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, SPHINCS+.

İkinci aşamaya geçmeye hak kazanan 26 sistemin İmzalama, Şifreleme ve Anahtar Paketleme kategorilerine göre kuantum sonrası güvenilir açık anahtarlı kriptosistem sınıflarına sayısal olarak dağılımı Tablo 5.7'de özetlenmiştir [3].

Tablo 5.6. NIST'e Gönderilen Kafes Tabanlı Sistemlerin Parametre Kümeleri

	Zor Problem	Sistem	n	q	σ	Gizli Dağılım	ϕ	Güvenlik Seviyesi
İmzalama Sistemleri	RLWE	qTESLA	1024	8058881	8.49	normal	x^n+1	AES 128-bit
			2048	27627521	8.49	normal	x^n+1	AES 256-bit
	NTRU	FALCON	512	12289	4.05	normal	x^n+1	AES 128-bit
			768	18433	4.05	normal	$x^n-x^{n/2}+1$	SHA 256-bit, AES 192-bit
		pqNTRUSign	1024	65537	0.70	((-1,1),501)	x^n-1	AES 128-bit, SHA 256-bit, AES 192-bit, SHA 384-bit, AES 256-bit
	MLWE, MSIS	CRYSTALS-DILITHIUM	768	8380417	3.74	(-6,6)	$x^{n/3}+1$	AES 128-bit
			1024	8380417	3.16	(-5,5)	$x^{n/4}+1$	SHA 256-bit
Şifreleme ve Anahtar Paketleme Sistemleri	RLWE	Ding Key Exchange	512	120883	4.19	normal	x^n+1	AES 128-bit
			1024	120883	2.60	normal	x^n+1	AES 192-bit, AES 256-bit
	NTRU	NTRU-HRSS-KEM	700	8192	0.79	((-1,1),437)	$\sum_{i=0}^{n-1} x^i$	AES 128-bit
	MLWE, MSIS	KINDI	768	16384	2.29	(-4,4)	$x^{n/3}+1$	SHA 256-bit
			1024	8192	1.12	(-2,2)	$x^{n/2}+1$	SHA 384-bit
	LWE	LOTUS	576	8192	3.00	normal	-	AES 128-bit, SHA 256-bit
			704	8192	3.00	normal	-	AES 192-bit, SHA 384-bit
	MLWE	CRYSTALS-KYBER	512	7681	1.58	normal	$x^{n/2}+1$	AES 128-bit
			768	7681	1.41	normal	$x^{n/3}+1$	AES 192-bit
	LWR	uRound2.PKE	500	32768	4.61	((-1,1),74)	-	AES 128-bit
			835	32768	2.29	((-1,1),166)	-	AES 256-bit

Tablo 5.7. NIST Çağrısı İkinci Aşamaya Geçen Kriptosistemlerin Sınıflandırılması

	Kod Tabanlı Kriptografi	Özet Tabanlı Kriptografi	Kafes Tabanlı Kriptografi	(İkinci Dereceden) Çok Değişkenli Polinom Sistemleri	Diğer	Toplam
İmzalama	-	1	3	4	1	9
Şifreleme ve Anahtar Paketleme	7	-	9	-	1	17
Toplam	7	1	12	4	2	26

Tablo 5.7'de kriptosistem sınıflarına dağılımı gösterilen toplam 26 başvurudan 12 tanesi kafes tabanlı kriptosistemlerden oluşmaktadır. İkinci aşamaya geçmeye hak kazanan kafes tabanlı kriptosistemler şu şekilde sınıflandırılabilir:

- **Şifreleme ve Anahtar Paketleme Sistemleri:**
  CRYSTALS-KYBER, FrodoKEM, LAC, NewHope, SABER, NTRU (NTRUEncrypt/NTRU-HRSS-KEM birleşimi), NTRU Prime, Round5 (Hila5/Round2 birleşimi), Three Bears.
- **İmzalama Sistemleri:**
  CRYSTALS-DILITHIUM, FALCON, qTESLA.

5.4. Değerlendirmeler

Kuantum mekaniğini temel alarak günümüz hesaplama sistemleri için zor olan matematiksel problemleri çözebilecek olan kuantum bilgisayarların üretilmesi veya üretilebilecek olması ihtimali Shor algoritması varlığında günümüzde kullanılan açık anahtarlı şifreleme sistemlerini güvensiz hale getirecektir. Bu durum ise kuantum bilgisayarların varlığında güvenilir sistemlerin nasıl oluşturulabileceği sorusuna neden olmuştur. Zor kafes problemlerini çözmek için kuantum bilgisayarlarda polinom zamanda çalışan bir algoritma bilinmediği için kafes tabanlı kriptosistemler kuantum sonrası için güvenilir bir sistem olarak değerlendirilmektedir. Bu çalışmada kuantum sonrası bilgisayarların varlığında güvensiz hale gelecek olan sistemler için

önerilen güvenilir alternatiflerden bahsedilmiştir. Bu kapsamda kuantum bilgisayarlar sonrası kafes tabanlı kriptosistemlerin tarihsel gelişiminden bahsedilerek bu sistemlerin güvenlik garantisi olarak değerlendirilen temel zor kafes problemleri açıklanmıştır. Ayrıca bazı zor kafes problemleri arası ilişkiler yorumlanmıştır.

Son olarak, zor kafes problemlerinden bazıları temel alınarak oluşturulan, kuantum bilgisayarlar sonrası standartlaşma sürecinde kendine yer bulan, kafes tabanlı kriptosistemlere yönelik değerlendirmelere yer verilmiştir.

Teşekkür

Bu çalışma EEEAG-117E636 proje numarası ile TÜBİTAK tarafından desteklenmiştir.

Kaynaklar

[1] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography, Springer, 2008.

[2] J. A. Buchmann, D. Butin, F. Göpfert, and A. Petzoldt, "Post-Quantum Cryptography: State of the Art. In The New Codebreakers," Springer, Berlin, Heidelberg, 2016, pp. 88-108.

[3] NIST Post-Quantum Cryptography Standardization Project, https://csrc.nist.gov/projects/post-quantum-cryptograph (Erişim Tarihi: 25.01.2019)

[4] P. Q. Nguyen, and J. Stern, "The two faces of lattices in cryptology. In Cryptography and Lattices," Springer, Berlin, Heidelberg, 2001, pp. 146-180.

[5] M. Ajtai, "Generating hard instances of lattice problems," in Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, ACM, July 1996, pp. 99-108.

[6] C. Peikert, "A decade of lattice cryptography," Foundations and Trends® in Theoretical Computer Science, 10(4), 2016, pp. 283-424.

[7] J. Hoffstein, J. Pipher, and J. H. Silverman, An introduction to mathematical cryptography, vol. 1 New York: Springer, 2008, pp. 373-453.

[8] D. P. Chi, J. W. Choi, J. San Kim, and T. Kim, "Lattice Based Cryptography for Beginners," IACR Cryptology ePrint Archive, 2015, pp. 938.

[9] D. Micciancio, and S. Goldwasser, Complexity of lattice problems: a cryptographic perspective, Springer Science and Business Media, vol. 671, 2012, pp. 185-187.

[10] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," In International Algorithmic Number Theory Symposium, Springer, Berlin, Heidelberg, June 1998, pp. 267–288.

[11] O. Goldreich and S. Goldwasser, "On the limits of nonapproximability of lattice problems," J. Comput. Syst. Sci., 60(3), 2000, pp. 540–563, Preliminary version in STOC 1998.

[12] O. Regev, "Lecture notes of lattices in computer science (Introduction)," Computer Science Department of Tel Aviv University, 2004.

[13] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," In Proc. 37th ACM Symp. on Theory of Computing (STOC), 2005, pp. 84–93.

[14] V. Lyubashevsky, C. Peikert and O. Regev, "On ideal lattices and learning with errors over rings," Journal of the ACM (JACM), 60(6), 2013, pp. 43.

[15] J. Lee, D. Kim, H. Lee, Y. Lee, and J. H. Cheon, "RLizard: Post-Quantum Key Encapsulation Mechanism for IoT Devices," IEEE Access, vol. 7, 2019, pp. 2080-2091.

[16] T. Plantard, W. Susilo, and K. T. Win, "A digital signature scheme based on CVP_{∞}," in International Workshop on Public Key Cryptography, Springer, Berlin, Heidelberg, March 2008, pp. 288-307.

[17] SageMath - Open-Source Mathematical Software System, http://www.sagemath.org/ (Erişim Tarihi: 25.01.2019)

[18] J.H. van de Pol., Lattice-based Cryptography, Eindhoven University of Technology Department of Mathematics and Computer Science, M. Sc. Thesis, 2011.

[19] L. Chen, S. Jordan, Y.K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "NISTIR 8105, Report on Post-Quantum Cryptography," National Institute of Standards and Technology (NIST), 2016.

[20] M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer, "Estimate all the {LWE, NTRU} schemes!," Cryptology ePrint Archive, Report 2018/331, 2018.

[21] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Software and Hardware Implementation of Lattice-based Cryptography Schemes," CECS TR 17-04, posted on November 9, 2017.

Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim

BÖLÜM 6

Dr. Mehmet Bedii KAYA

HUKUKİ AÇIDAN BİLİŞİM SUÇLARI, SİBER GÜVENLİK VE ADLİ BİLİŞİM

6.1. Giriş

Dünyada siber güvenlik tehditleri artmakta, şekil ve nitelik değiştirmekte, bu tehditlerin etkilediği alanlar farklılaşmaktadır. Bu gelişime ve değişime bağlı olarak da bilişim suçları çok farklı şekilde işlenmekte; bilişim suçlarına konu fiil ve eylemler geniş bir spektruma yayılmaktadır. Nitekim, hacker olarak adlandırılan bilişim suçluları meydan okuma, ego, isyan, kazanç elde etme gibi amaçlarla; suçlular ve kiralık saldırganlar, bilginin yok edilmesi ya da parasal kazanç amaçlarıyla; teröristler, devletler ve devlet dışı aktörler, yok etme, istismar, intikam, hükümetlerin yıkılması, bölgesel veya küresel ticaretin bozulması gibi amaçlarla; endüstriyel casuslar, rekabette avantaj, ekonomik casusluk veya maddi kazanç elde etme amaçlarıyla; iç tehdit olarak adlandırılan kişi veya kişi grupları ise, ego, merak, parasal kazançlar, intikam hissi veya istihbarat gibi amaçlarla siber saldırılar düzenlemektedir [1].

Sadece bireysel suçlular değil, suç örgütleri, devlet dışı aktörler ve devletler de mevcut açıkları kullanmakta ve hatta kendileri özel açıklar ve araçlar geliştirmektedir. Bilişim suçları; bilişim sistemine girme, botnet kullanma, DDoS saldırıları, siber takip, ağ izleme (sniffing), aldatma (spoofing), bilgi çalma, özel veriye yetkisiz erişim, sabotaj başta olmak üzere çok geniş yelpazede fiil ve hareketlerle işlenmektedir.

Bilişim sistemlerinin nitelik ve nicelik olarak gelişmesi, değişmesi ve farklılaşması, bu suçların hem işleniş şekillerini hem de adli bilişim bağlamında incelenmesini girift hale getirmiştir. Öyle ki, her bir bilişim sistemi için farklı adli bilişim tekniklerinin kullanılması zaruri hale gelmiş; adli bilişim, bilgisayar, ağ, veritabanı, bulut, mobil, araç, IoT adli bilişimi gibi alt kırılımlara uğramıştır. Veri kaydedile-

bilen ortamlardaki esaslı değişiklikler, bu alandaki mevcut kuralların da kapsamlı şekilde gözden geçirilmesini zorunlu kılmaktadır.

Bilişim suçlarının sınır aşan niteliği, bilişim sistemlerinin hızla gelişmesi, hayatın farklı alanlarında farklı amaçlarla kullanılmaya başlanması, teknoloji ve hukuk arasındaki etkileşimde önemli bir kırılma noktası olmuş; bu alanda çıkan uyuşmazlıkların soruşturulması ve kovuşturulması sui generis bir nitelik kazanmıştır. Bu çalışmanın amacı bilişim suçlarının Türk hukukunda nasıl düzenlendiğini incelemek, bu konudaki güncel sorunları tespit etmek ve yasal çerçevenin bilişim ve teknolojideki gelişmelere ne kadar yanıt verebildiği sorusuna cevap bulmaktadır. Çalışma, dört ana bölüme ayrılmıştır. İlk bölümde Türk hukukunda bilişim suçları, ikinci bölümde hukuki açıdan siber güvenlik, üçüncü bölümde ise adli bilişim konuları incelenecek olup, son bölümde değerlendirmelere yer verilecektir.

6.2. Bilişim Suçları

5237 sayılı Türk Ceza Kanunu'nun Özel Hükümler isimli İkinci Kitap'ının "Topluma Karşı Suçlar" başlıklı Üçüncü Kısım'ının Onuncu Bölümü "Bilişim Alanında Suçlar"a ayrılmıştır. Bu doğrultuda Bilişim sistemine girme (Madde 243), Sistemi engelleme, bozma, verileri yok etme veya değiştirme (Madde 244), Banka veya kredi kartlarının kötüye kullanılması (Madde 245), Yasak cihaz veya programlar (Madde 245A) ve Tüzel kişiler hakkında güvenlik tedbiri uygulanması (Madde 246) madde başlıklı beş farklı maddeyle bilişim alanını ilgilendiren en önemli fiil ve hareketler suç kapsamına alınmıştır. Bu suçların, bilişim sistemlerinin güvenliği, sistemin manipüle edilmeden doğru bir şekilde işlemesi, içerdiği verilerin bütünlüğü, sıhhati, sistem içerisinde kredi kartlarının kullanılma yoğunluğu ve ekonomik sistemdeki rolü nedeniyle; bu sistemlerin kötüye kullanılmasının önlenmesi, toplumdaki herkesin yararına olacağı için "Topluma Karşı Suçlar" kısmında düzenlenmiştir [2].

Suçlar, zaman içerisinde bilişim alanındaki gelişmelerle uyumlu şekilde gelişmiş ve yeni suç tipleri ihdas edilmiştir. 2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesiyle Türk Ceza Kanunu'na eklenen 245A maddesinde yer alan yasak cihaz veya programlar suçu güncel bir örnektir. Benzer şekilde, 6698 sayılı Kanun'un 30. maddesiyle Türk Ceza Kanunu'nun 243. maddesine

eklenen dördüncü fıkrada kendine yer bulan veri nakillerini sisteme girmeksizin izleme suçu da toplumsal bir ihtiyaca cevap vermek adına ihdas edilmiştir.

Bilişim sistemlerini ilgilendiren suçlar sadece bu bölümde düzenlenen suçlar değildir. Türk Ceza Kanunu'nun başka bölümlerinde de bilişim sistemlerini ilgilendiren, bilişim sistemlerini kullanarak haksız yarar sağlamayı veya bilişim sistemlerinin bir aracı olarak kullanılmasını farklı şekilde yaptırıma bağlayan hükümler yer almaktadır. "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı Dokuzuncu Bölümde yer alan Kişisel verilerin kaydedilmesi (Madde 135), Verileri hukuka aykırı olarak verme veya ele geçirme (Madde 136), Verileri yok etmeme (Madde 138) suçları dışında, Türk Ceza Kanunu'nun çeşitli bölümlerinde, Haberleşmenin gizliliğinin ihlali suçu (Madde 132), Hakaret (Madde 125), Haberleşmenin engellenmesi suçu (Madde 124), Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (Madde 142/2-e), Bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu (Madde 158/1-f) gibi bilişim sistemleriyle işlenmesi mümkün çeşitli suçlar da yer almaktadır.

Bu çalışma kapsamında klasik bilişim suçları olarak nitelendirilebilecek temel bilişim suçları incelenecek; bilişim sistemlerini ilgilendiren veya bilişim sistemleriyle işlenmesi mümkün suçlara ise ilgili yerlerde değinilecektir. Banka veya kredi kartlarının kötüye kullanılması suçu inceleme kapsamına alınmamıştır. İlgili suçlar incelenmeden önce, konunun uluslararası hukuktaki en önemli ve kapsayıcı düzenlemesi olan Avrupa Konseyi Siber Suç Sözleşmesi kısaca incelenecektir.

6.2.1. Avrupa Konseyi Siber Suç Sözleşmesi

Bilişim suçlarının coğrafi sınır tanımaması, çok az masrafla çok kısa sürede büyük zararlara yol açabilecek şekilde işlenmesi ve faillerin, çoğu zaman bu suçlarda anonim olması nedeniyle bu suçlarla mücadelede devletlerin iş birliği yapması kaçınılmaz olmuştur. Özellikle, bu suçların çoğu zaman sınır aşan şekilde işlenmesi, hangi ülkenin yargısının yetkili olacağına ilişkin olarak adli yardımlaşmayı gerekli kılmaktadır. Söz konusu nedenlerle bilişim suçları ile mücadelede Birleşmiş Milletler, Avrupa Konseyi, Avrupa Birliği, OECD,

G8 gibi uluslararası kuruluşlar birçok çalışma yürütmüştür. Bu çalışmalar arasında Avrupa Konseyi Siber Suç Sözleşmesi'ni diğerlerinden ayıran husus, sözleşmeye taraf devletlerin, bilişim suçlarına ilişkin olarak iç hukuklarında düzenleme yapmayı ve uluslararası adli iş birliğini taahhüt etmiş olmalarıdır. Sözleşme, her ne kadar Avrupa Konseyi nezdinde imzalanmış olsa da konsey üyesi olmayan ve aynı zamanda Avrupa kıtası dışında bulunan ABD, Kanada, Japonya, Güney Afrika, İsrail, Avusturalya gibi ülkelerin de taraf olması nedeniyle bölgesel değil uluslararası bir nitelik arz etmektedir.

Avrupa Konseyi, bu sürece, konseyin alt çalışma komitelerinden birisi olan Avrupa Suç Sorunları Komitesi'nin (The European Committee on Crime Problems) 1996 yılında siber suçlarla ilgilenecek bir uzmanlar komitesi kurulmasını önermesi ile başlamıştır [3]. 1997 yılında Avrupa Konseyi Bakanlar Kurulu, söz konusu uzmanlar komitesini (Committee of Experts on Crime in Cyberspace) kurmuş ve komiteden siber suçlarla mücadeleye ilişkin bağlayıcı özelliğe sahip bir hukuki metin hazırlamasını istemiştir. Bunun üzerine komitenin hazırladığı taslak metin, 23 Kasım 2001'de Macaristan'ın başkenti Budapeşte'de imzaya açılmıştır. Türkiye sözleşmeyi 10 Kasım 2010 tarihinde imzalamış, 29 Eylül 2014 tarihinde onaylamış ve sözleşme, 1 Ocak 2015 tarihinde iç hukuk bağlamında yürürlüğe girmiştir [4]. 8 Ekim 2018 tarihi itibariyle sözleşmeye taraf 61 ülke bulunmaktadır ve bu ülkelerin on sekizi Avrupa Konseyi üyesi değildir [5].

Sözleşme, 48 madde ve dört bölümden müteşekkildir. Bu bölümler sırasıyla; terimler, ulusal düzeyde alınacak önlemler, uluslararası iş birliği ve diğer hükümler şeklindedir. Terimler bölümünde; bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik verisi terimleri tanımlanmıştır. Ulusal düzeyde alınacak önlemlerden bir kısmı maddi ceza hukukuna ilişkin iken bir kısmı muhakeme hukukuna ilişkindir. Maddi ceza hukukuna ilişkin kısımda taraf devletlerin hangi fiilleri iç hukukları bakımından suç olarak kabul edeceği belirtilmiştir. Muhakeme hukukuna ilişkin kısımda ise, özellikle bilişim suçlarında, suç delillerine ulaşmanın ve mahkeme önünde temsil edici, bütünlüğü bozulmamış delil elde etmenin zorluğu nedeniyle ulusal hukuklara yön gösterici hükümler getirilmiştir. Uluslararası iş birliği bölümünde ise uluslararası adli yardımlaşmaya ilişkin hükümler bulunmaktadır.

Avrupa Konseyi Siber Suç Sözleşmesi'nde tanımlanan ve taraf devletlerin iç hukuklarına dahil etmeleri gereken suç tipleri şu şekilde sıralanabilir:

- Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar başlığında düzenlenen suçlar: Yasadışı erişim, yasadışı araya girme, verilere müdahale, sisteme müdahale, cihazların kötüye kullanımı (Madde 2-6)
- Bilgisayarla bağlantılı suçlar başlığında düzenlenen suçlar: Bilgisayarla bağlantılı sahtecilik, bilgisayarla bağlantılı dolandırıcılık (Madde 7-8)
- İçerikle bağlantılı suçlar başlığında düzenlenen suçlar: Çocuk pornografisiyle bağlantılı suçlar (Madde 9)
- Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar (Madde 10).

6.2.2. Bilişim Sistemine Girme veya Sistemde Kalma Suçu

Türk Ceza Kanunu'nun 243. maddesi şu şekildedir:

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.

Bilişim sistemine girme veya sistemde kalma suçu kapsamında ilk fıkrada suçun temel hali; ikinci fıkrada suçun daha az cezayı gerektiren nitelikli hali; üçüncü fıkrada ise suçun neticesi sebebiyle ağırlaşan şekli düzenlenmiştir. 2016 yılında ise, ilgili maddeye ayrı

bir dördüncü fıkra eklenmek suretiyle müstakil bir suç niteliğinde olan veri nakillerini sisteme girmeksizin teknik araçla izleme suçu düzenlenmiştir.

Bilişim sistemine girme suçu, Avrupa Konseyi Siber Suç Sözleşmesi'yle uyumlu bir düzenlemedir. Sözleşmenin 2. maddesinde "*Her bir taraf devlet, bir bilgisayar sisteminin tamamı veya herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yapmalı, gerekli önlemleri almalıdır. Taraf devlet, bu suçun oluşması için erişimin güvenlik önlemleri ihlal edilerek ya da bilgisayar sistemine bağlı diğer bir bilgisayar sistemi aracılığıyla bilgisayar verisini almak ya da başka kötü niyetlerle kullanmak şartına bağlayabilir.*" hükmü yer almaktadır. Türk Ceza Kanunu'nun 243. maddesinin birinci fıkrasında tanımlanmış olan bilişim sistemine girme suçu, Avrupa Konseyi Siber Suç Sözleşmesi'nde yer alan her bir taraf devletin bir bilgisayar sisteminin tamamına veya herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yaparak gerekli önlemleri almasını öngören yükümlülüğü karşılamaktadır. Bilişim sistemine girme suçunun oluşması, erişimin, güvenlik önlemleri ihlal edilerek ya da bilgisayar sistemine bağlı diğer bir bilgisayar sistemi aracılığıyla bilgisayar verisini almak ya da başka kötü niyetlerle kullanmak şartına bağlanmamıştır [6].

6.2.2.1. Korunan Hukuki Değer

Bilişim sistemine girme veya sistemde kalma suçunda birden fazla hukuki değer korunmaktadır ve bu değerler, bilişim sistemlerinin güvenliği ve güvenilirliğidir [7]. Haklı olarak belirtildiği üzere bilişim sistemlerinin güvenliği, verilerin gizliliğinin korunmasından, özel hayatın dokunulmazlığına, kişilerin veya kurumların ihtiyaç duyduğu güvenlik duygusundan öte, üstün bir değerdir [8]. Bilişim sistemlerinin sağlıktan güvenliğe, eğitimden bankacılığa, evlerden işyerlerine, devletten özel sektöre, gençlerden yaşlılara kadar çok farklı alanlarda, yerlerde ve kişilerce kullanılıyor olması, bunların güvenliğinin sağlanması için özel bir düzenleme yapılmasını gerektirmiştir. Bilişim sistemlerinin güvenilirliği ise toplumda bu sistemlere karşı oluşan güven duygusunu; kişilerin kendilerine özgü ve sadece kendilerinin yönetmek isteyecekleri bir alan oluşturduklarını; bu sebepledir ki bu alanın kişiliklerini rahatlıkla geliştirebile-

cekleri güvenli bir alan olmasını isteme ve bu güvenliğin korunmasını bekleme hakkına sahip olduğunu ifade etmektedir [9]. Bilişim sistemlerinin güvenilirliğinin korunmasının korunan hukuki değer olduğunun bir dayanağı olarak da bilişim alanında işlenen suçların, topluma karşı işlenen suçlar kapsamında düzenlenmiş olması ve bu bilişim sistemlerine karşı toplumda ortaya çıkan güven duygusunun korunması ihtiyacı olduğu gösterilmektedir.

Hem bireyler hem de devlet bilişim sistemlerine güvenmektedir. Bireyler, paralarını bilişim sistemlerine emanet etmekte, en hassas ve özel hayatlarının en mahrem verilerini bilişim sistemlerine kaydetmekte, bilişim sistemleri aracılığıyla verileri aktarmaktadır. Özellikle, internetin yaygınlaşmasıyla bilişim sistemlerinin kullanımı farklı bir evreye ulaşmıştır. İnternet kullanmak bir lüks olmaktan çıkmış ve artık, temel bir yetenek halini almıştır. Bu sebeple, interneti kim kullanıyor sorusuna tüketici bir yanıt vermek zorlaşmakta; aynı şekilde, internetin etkileşimli özelliği, internetin kullanım alanları için tüketici bir listeleme yapmayı imkânsız kılmaktadır.

Bilişim sistemleri kamu tarafından da yaygın şekilde kullanılmaktadır. Öyle ki, bazı ülkelerde seçimler veya referandumlar bile bilişim sistemleri aracılığıyla gerçekleşebilmektedir [10]. Ayrıca, kamu hizmetlerinin dijital ortamda sunulması veya kamu hizmetlerinin sunumunda bilişim sistemlerinden faydalanılması artık istisna değil, asıl olmuştur. Kamu hizmetlerinin ilk önce e-Devlet hizmeti olarak tasarlanması veya mevcut hizmetlerin ağırlıklı olarak elektronik ortamdan yürütülecek şekilde modernizasyonunun sağlanması ("Digital by default" ilkesi) ile e-Devlet hizmetlerinin tek işlem veya başvuru ile tamamlanabilmesini sağlayacak şekilde geliştirilmesi prensipleri ("Once only principle" ilkesi) çeşitli strateji belgelerinde ve hukuki düzenlemelerde yer bulmuştur [11]. Türkiye'de de e-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik, e-Devlet hizmetlerinin kesintisiz ve kaliteli hizmet sağlanmasını, bilgi ve iletişim teknolojilerinin kullanımının yaygınlaştırılmasını ve bilişim sistemlerinin güvenliğine yönelik ulusal ve uluslararası standartlara uyulmasını, tüm kamu kurum ve kuruluşlarının, e-Devlet projelerinin hayata geçirirken ve sunarken uyması gereken temel ilkeler olarak belirlemiştir [12]. Bu açık normatif dayanak ve bireylerin yukarıda izah edilen bilişimi kullanma alanları dikkate alındığında bilişim sistemlerinin güvenilirliğinin,

bilişim sistemlerinin güvenliği kadar; hatta onun da önüne geçen bir hukuki değer olduğu söylenebilir.

6.2.2.2. Tipikliğin Maddi Unsurları

Her suçun bir kanuni tanımı vardır ve bu tanım suçu soyut olarak tanımlar. Bu çizilen soyut çerçeve veya şablon somut olaya uygulanmak suretiyle suçun varlığı tespit edilir. Her suç, aslında bir yazılım gibi değişkenler, döngüler, fonksiyonlar, koşul yapıları, diziler ve algoritmalar şeklinde formüle edilebilir. Yazılımcı sıfatıyla kanun koyucu programı yazar; yargı ise somut bir uyuşmazlıkta verileri girerek, değişkenleri tanımlayarak programı çalıştırır ve bir karara varır. Elbette uyuşmazlıklar, her zaman steril ve de basit değildir. Uyuşmazlıkların belirli aşamalarında, yani belirli döngülerin sonunda, hâkimin müdahale etmesi, vicdanına ve muhakemesine dayalı olarak bir tercihte bulunması ve nihayetinde bir karar vererek bir sonraki döngüye geçmesi gerekir.

Bilişim sistemine girme veya sistemde kalma suçunda suçun kanuni unsuru, yani tipiklik, çeşitli alt unsurlardan oluşmaktadır.

a. Fail

Bilişim sistemine girme veya sistemde kalma suçu herkes tarafından işlenebilecek bir suçtur. Bu suç için özel bir nitelik aranmamaktadır. Bilişim sistemine girme veya sistemde kalma suçunun işlenebilmesi için gerekli olan teknik bilgi, her bilişim sistemi için farklıdır. Bilişim sistemleri o kadar çeşitlenmiş ve hayatın o kadar farklı alanlarında kullanılmaktadır ki, her bilişim sistemi için farklı bir yöntem ve teknik gerekmektedir. Fail, bilişim sistemine girmek için gerekli kodu/uygulamayı kendi geliştirebileceği gibi, başkasının yazdığı bir kodu/uygulamayı da kullanabilir. Bilişim sistemine girme suçunun failleri hacker, cracker, phreaker veya lamer gibi farklı sıfatlarla anılabilir. Aşağıda açıklanacağı üzere, salt kodun/uygulamanın, yasak cihaz ve programların geliştirilmesi müstakil suç olarak tanımlanmıştır. İş birliği durumları suçun özel görünüş hallerinde suçluların çokluğu (iştirak) kısmında ayrıca açıklanacaktır.

Öte yandan, şunu da belirtmek gerekir ki, bilişim sistemine girme veya sistemde kalma suçunun işlenebilmesi için gerekli olan teknik bilgiler internet ortamında kolaylıkla erişilebilir yerlerde de bulu-

nabilmektedir. Karmaşık sistemlerin de bazen o kadar temel açıkları vardır ki, teknik yeterliği olmayan, temel seviyede bilgisayar kullanan birisi bile bilişim sistemine girme suçunun faili olabilir. Sisteme kolay veya zor girilmiş olması, suçun oluşması ve fail olmak bakımından önem arz etmemektedir.

Bilişim sistemine girme veya sistemde kalma suçunun faili tüzel kişi olabilir mi? Tüzel kişilerin suç faili olamayacakları ve ceza sorumluluklarının bulunmadığı; ancak, bilişim sistemine girme veya sistemde kalma suçu işlenmesi suretiyle bir tüzel kişinin yararına haksız menfaat sağlanmışsa, Türk Ceza Kanunu'nun 246. maddesi uyarınca bunlara özgü güvenlik tedbirleri uygulanabileceği kabul edilmektedir [13].

b. Mağdur

Türk Ceza Kanunu, fail gibi mağdur açısından da bilişim sistemine girme veya sistemde kalma suçunda özel bir şart aramamıştır. Herkes bu suçun mağduru olabilir. Suçun mağduru kimdir sorusunun yanıtında ise, bilişim sistemi üzerinden hak sahibi olma kriterinden hareket edilmektedir [14]. Teknik olarak yetkilendirmeden hareketle; diğer bir deyişle kimin bilişim alanına izinsiz giriş sağlandığından yola çıkarak mağdurun kim olduğu tespit edilecektir. Sistem üzerinde bir kişi hak sahibi olabileceği gibi; diğer bir deyişle, mağdur olabileceği gibi birden çok kişi de yetkilendirilmiş ve dolayısıyla mağdur olabilir [15]. Mağdurun açık veya örtülü rızası halinde suç oluşmayacaktır. Rıza konusu, hukuka aykırılık unsurunda etraflıca incelenecektir. Tüzel kişiler suçun mağduru olabilir mi? Bilişim sistemine girme veya sistemde kalma suçunun mağduru ancak gerçek kişiler olabilir; tüzel kişiler ise suçtan zarar gören olarak nitelendirilecektir [16].

Bilişim sistemine girme veya sistemde kalma suçunun konusu olan bilişim sisteminde hiçbir güvenlik önleminin alınmamış olmasının suçun oluşmasına veya cezaya etkisi var mıdır? Bilişim sisteminde güvenlik önlemi alınmamış olmasının suçun oluşmasına veya cezaya etkisi olmadığı gibi; özel nitelikli kişisel veriler gibi hassas veya kritik verilerin barındırıldığı bilişim sistemlerine girme veya sistemde kalma hallerinin, suçun cezasının arttıran nitelikli hal olarak düzenlenmesi gerektiği tartışılmaktadır [17]. Esasında, güvenlik önlemi göreceli bir kavramdır. Her sistem için alınabilecek farklı

nitelikte ve seviyede tedbirler vardır. Hukuki belirlilik açısından güvenlik önlemini esas alarak hareket etmek, bu sebeple yerinde olmayacaktır.

c. Suçun Konusu

Bilişim sistemine girme veya sistemde kalma suçunun konusu Türk Ceza Kanunu'nun 243. maddesindeki her bir fıkra için farklıdır. Bilişim sistemine girme suçunun düzenlendiği birinci fıkrada suçun konusu hukuka aykırı olarak girilen veya kalınan bilişim sistemi; nitelikli halini düzenleyen ikinci fıkrada suçun konusu, bedeli karşılığı yararlanılabilen sistemler ve üçüncü fıkrada düzenlenen netice sebebiyle ağırlaşan halde ise bilişim sisteminde yer alan verilerdir. Her ne kadar hukuki değer ve suçun konusu birbiriyle yakın ve hatta bazı durumlarda iç içe geçmiş kavramlar olsa da, müstakil ve farklı kavramlardır [18]. Bir suçta korunan hukuki değer, eylemle ihlal edilen hukuki varlık veya menfaati ifade etmektedir; suçun konusu ise eylemin yöneldiği kişi veya şeydir [19].

243. maddenin gerekçesinde bilişim sistemi, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler olarak tanımlanmıştır [20]. Üçüncü fıkrada suçun konusu olan veri kavramı Türk Ceza Kanunu'nda açıkça tanımlanmamış olsa da, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2. maddesinin birinci fıkrasının (k) bendinde bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer olarak tanımlanmıştır. Bu tanım sadece yol gösterici nitelikte olup, bilişim sistemine girme veya kalma suçu için yerindeliği tartışılabilir.

Önemle belirtmek gerekir ki, bütününe veya bir kısmına, hukuka aykırı olarak girilen veya orada kalınmaya devam edilen sistem bir bilişim sistemi değilse, Türk Ceza Kanunu'nun 243. maddesinin birinci fıkrasında yer alan suç oluşmayacaktır. Türk Ceza Kanunu gerekçesinde yer alan tanım, şüphesiz, bağlayıcı değildir ve sadece yol göstericidir. Bir bilişim sisteminden bahsedilebilmesi için, ortada verileri toplayabilme, saklayabilme, işleyebilme, çoğaltabilme, değerlendirebilme ve aktarabilme özelliklerine sahip olan ve bu fonksiyonları, çok yönlü olarak otomatik işlemlere tabi tutma olanağı veren bir sistemin varlığının gerekliliği ileri sürülmektedir

[21]. Peki gelişen teknolojiler karşısında bilişim sistemi nasıl tanımlanmalıdır? Bilişim sistemi kavramı bilgisayarlardan ibaret değildir. Salt bilgisayar olarak nitelendirilmesi suçun kapsamını aşırı sınırlayacağı gibi, korunan hukuki değerler dikkate alındığında amaca uygun düşmeyecektir. Bu sebepledir ki, bilgisayarların yanı sıra bilgisayar olarak nitelendirilmemesine rağmen veri iletişimi sağlayan bilişim alanına dahil unsurlardan sayılması gereken diğer elektronik, manyetik, mekanik araçlar üzerinde veyahut bunları, veri iletişimi için birbirine bağlayan somut veya soyut ağlar üzerinde işlenebileceği kabul edilmektedir [22]. Bilgisayar, dizüstü bilgisayar, tablet, elektronik kitap okuyucu, akıllı saatler, ağ cihazları ve eşyaların interneti altında genel olarak sınıflandırılabilecek akıllı cihazlar, bilişim sistemine hukuka aykırı girme veya sistemde kalma suçunun konusu olabilecektir [23]. Nitekim, eşyaların internetiyle bilişim sistemleri günlük hayatın çok geniş alanlarına girmiş, bilişim sistemlerinin birbiriyle etkileşimleri artmış ve bu sebepledir ki, bunların güvenliğinin ve güvenilirliğinin korunmasında üstün toplumsal bir fayda ortaya çıkmıştır. Dolayısıyla, korunan hukuki değerler ve toplumsal menfaatler dikkate alındığında, bilişim sistemi kavramının mümkün olduğunca geniş yorumlanması yerinde bir yaklaşım olacaktır.

ç. Hareket

Bilişim sistemine girme suçunun oluşması için hangi tür yöntem veya teknik kullanılırsa kullanılsın asıl olan bilişim sistemine girme veya sistemde kalma fiilleridir. Bilişim sistemine girme eylemi veya sistemde kalma eylemlerinden birisinin yerine getirilmesi durumunda suç oluşmaktadır. Sisteme girme veya sistemde kalma fiillerinin cezalandırılmaları bakımından fark var mıdır? Kanun koyucu bu konuda bir ayrıma gitmemiş olup her iki fiilin de cezası aynıdır: bir yıla kadar hapis veya adli para cezası [24]. Hem sisteme girilmesi hem de sistemde kalmaya devam edilmesi durumunda cezalandırılma nasıl olacaktır? Bu tür durumlarda tek suçun bulunduğunun kabul edilmesi yerinde olacaktır [25]. Zira girme ve kalma hareketleri kanunda seçimlik olarak düzenlenmiştir.

Bilişim sistemine girildiği ancak sistemdeki hiçbir veriye veya dosyaya dokunulmadığı; verinin aktarılmadığı durumlarda suç oluşacak mıdır? Bilişim sistemine girme suçu, aynı zamanda soyut teh-

like suçudur. Somut tehlike suçlarında, zarar tehlikesinin gerçek olması gerekirken; soyut tehlike suçlarında ise hareketin yapılmış olması yeterli olup, ayrıca somut bir tehlikenin meydana gelmesine gerek yoktur [26]. Bilişim sistemine girme veya sistemde kalma suçunun oluşması için de bilişim sistemine girme veya sistemde kalma hareketlerinden birisinin yerine getirilmesi suçun oluşması için yeterlidir; zararın oluşması ya da zararın doğması için somut veya yakın bir tehlikenin oluşması gerekmemektedir [27].

Bilişim sistemine girme suçu ne zaman oluşur? Bilişim sistemine girmek olarak hüküm kaleme alındığı için bundan yola çıkarak girmek fiili; donanıma fiziksel olarak girilmesi olarak mı, yoksa yazılıma erişilmesi olarak mı anlaşılmalıdır? Bilişim sisteminin oluşturduğu soyut alana girildiği an; sistemin tamamına veya bir kısmına ulaşmak, içeriğine dahil olmak; bu doğrultuda yazılım alanına girilmesiyle suçun işlendiği kabul edilmektedir [28]. Diğer bir deyişle, bilişim sistemlerinin oluşturduğu sanal alana girilmesi gerekir [29]. Aynı doğrultuda, suçun oluşması için, sisteme girişi engelleyici tedbirlerin alınmış olması şart kabul edilmemektedir [30].

Bilişim sistemine girme suçunun farklı yöntem ve teknikler kullanılarak işlenmesi mümkündür. Suçun oluşması için bir hukuki sınırın ihlal edilmesi yeterli görülmektedir [31]. İhlalin nasıl gerçekleştiği veya sisteme girmenin ne kadar zor veya kolay olduğu, sisteme giriş için kullanılan uygulamanın bizzat fail tarafından geliştirilmiş olmasıyla başka birisi tarafından geliştirilmiş bir uygulamanın kullanılması önemli değildir.

Hukuki bir sınır ihlal edilmemişse veya sisteme girilmesi için rıza söz konusuysa suç da oluşmayacaktır. Erişime yönelik bir kısıtlamanın olmadığı, herkesin erişebildiği veya örneğin belirli bir grubun erişimine açık olan bir bilişim sistemine yine bu gruptan kişilerce erişim sağlandığı durumlarda suç oluşmayacaktır. Örneğin, bir şirketin çalışanlarının doğrudan erişimine açtığı sisteme şirket çalışanlarının erişiminde suç oluşmayacakken; şirket tarafından izin verilenler dışında birilerinin erişimi durumunda suç oluşacaktır.

Türk Ceza Kanunu'nun 243. maddesinin ilk kabul edildiği 2004 yılındaki halinde bilişim sistemine girme suçu *"bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir"*

şeklindeydi. TBMM Adalet Komisyonu'nda her ne kadar "veya" bağlacı hali kabul edilmişse de TBMM Genel Kurulu'nda "veya" bağlayıcı, "ve" olarak değiştirilmiştir. Her ne kadar Türk Ceza Kanunu gerekçesinde *"maddenin birinci fıkrasında bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiili suç hâline getirilmiştir"* denilmiş olsa da "veya" değil, "ve" bağlacı şeklinde hüküm yürürlüğe girmiştir.

Açıkça "ve" bağlacıyla iki fiil birbiriyle bağlandığı için suçun oluşması için bilişim sisteminin bütününe veya bir kısmına hem hukuka aykırı olarak girilmesi ve hem de orada kalmaya devam edilmesi gerektiği gibi bir durum söz konusuydu [32]. Bu sebepledir ki, suç birden fazla hareketin birbirine bağlı şekilde yapılmasını gerektirdiği için birleşik hareketli bir suç olarak kabul edilmekteydi [33]. Bu dönemde en önemli tartışmalardan birisi suçun oluşması için sistemde ne kadar kalınması gerektiğiydi [34]. Haklı olarak belirtildiği üzere, suç konusunu oluşturan her bilişim sisteminin özelliği ve güvenlik yapısının birbirinden farklı olması başta olmak üzere sistemde kalma hareketinin hangi andan itibaren başladığının belirlenmesi, her somut olay açısından farklılık gösterdiği için farklı uygulamalara yol açmıştır [35]. Esasında Avrupa Konseyi Siber Suç Sözleşmesi de bilişim sistemine hukuka aykırı erişimi suçun oluşması için yeterli görmekte; ayrıca kalma unsurunu aramamaktadır. Tüm bu eleştiriler ve Avrupa Konseyi Siber Suç Sözleşmesi'yle olan farklılıklar dikkate alınarak 2016 yılında Türk Ceza Kanunu'nun 243. maddesinin birinci fıkrasında 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesiyle değişiklik yapılmış ve bu fıkrada yer alan "ve" ibaresi, "veya" şeklinde değiştirilmiştir. Neticede, suç, birleşik hareketli suç olmaktan çıkarılmıştır. Suçun oluşması için bilişim sistemine girilmesi veya kalınması fiillerinden herhangi birinin işlenmesi yeterlidir.

Bilişim sistemine girme ne kadar suç ise bilişim sisteminde kalmak da aynı ölçüde suçtur. Yukarıda da belirtildiği üzere, hem sisteme girilmesi hem de sistemde kalmaya devam edilmesi durumunda tek suçun bulunduğunun kabul edilmesi yerinde olacaktır. Örneğin, kişiye bilişim sistemine giriş izni verilmiştir ancak değişen hukuki ilişki sebebiyle giriş yetkisi kaldırılmıştır. Benzer şekilde, bilişim sisteminin güvenliği başkası tarafından kırılmıştır ve mevcut güvenlik önlemleri kaldırılmıştır. Tüm bu ihtimallerde bilişim

sisteminde kalmaya devam edilmesi durumunda söz konusu suç oluşacaktır. Aşağıda etraflıca incelenecek hukuka aykırılık unsurunun sınırları, bu suçun sınırının çizilmesi için yol gösterici olacaktır. Bu doğrultuda, bilişim sistemine girme suçu, hukuka uygun olarak giren kişinin (ki rızayla veya başka bir hukuka uygunluk sebebiyle girilmiş olmasının önemi yoktur), hukuka aykırı olarak sistemde kalmaya devam etmesi veya başkasının bilişim sistemine kastı olmaksızın yanlışlıkla giren bir kimsenin, durumu fark etmesine rağmen sistemde kalması; diğer bir deyişle suç teşkil etmeyen sisteme icrai hareketle girmenin ihmali şekilde sürdürülmesi şeklinde işlenebilir [36]. Örneğin, kişiye bilişim sistemine giriş izni verilmiştir, ancak değişen hukuki ilişki sebebiyle giriş yetkisi kaldırılmıştır. Benzer şekilde, bilişim sisteminin güvenliği başkası tarafından kırılmıştır ve mevcut güvenlik önlemleri kaldırılmıştır. Tüm bu ihtimallerde, bilişim sisteminde kalmaya devam edilmesi durumunda söz konusu suç oluşacaktır. Aşağıda etraflıca incelenecek hukuka aykırılık unsurunun sınırları, bu suçun sınırının çizilmesi için yol gösterici olacaktır.

d. Suçun Bedeli Karşılığı Yararlanılabilen Sistemler Hakkında İşlenmesi

Bilişim sistemine girme veya sistemde kalma suçunun nitelikli hali Türk Ceza Kanunu'nun 243. maddesinin ikinci fıkrasında düzenlenmiştir. Nitelikli hal, suçun konusu olan bilişim sisteminin türüne göre belirlenmiştir. Söz konusu hükme göre, bedeli karşılığı yararlanılabilen bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girilmesi veya orada kalmaya devam edilmesi durumunda verilecek ceza yarı oranında indirilecektir.

Bedeli karşılığı yararlanılabilen bir bilişim sistemine yönelik getirilen indirimi yerinde görenler olduğu gibi eleştirenler de vardır. Söz konusu durumun indirim hali değil, ağırlaştırılmış hal olması gerektiği ileri sürülmektedir. Ceza indirimini yerinde görenler, hak sahibinin bedeli ödendiği takdirde sisteme girilmesine izin vermesi durumunda, bedeli ödeyenler bakımından sistemin güvenliğinden vazgeçilmekte; bu sebeple de bedel ödenerek girilen bir sisteme müdahalenin oluşturduğu haksızlık içeriği hiçbir şekilde girilmesine izin verilmeyen sisteme göre çok daha az olduğunu ileri sürmek-

tedir [37]. Ceza indirimini yerinde görmeyenler ise tek bir hukuksal değer ihlal edildiğinde bir birim ceza veriliyor iken, iki farklı hukuksal değerin ihlali halinde iki birim cezanın verilmesi gerektiğini; bedeli karşılığı yararlanılabilen sistemler hakkında suç işlenmesi halinde hem sistemin güvenliği hukuksal değerinin hem de bir şekilde sistemin sahibi veya ilgilisinin malvarlığının korunmasına yönelik hukuksal değerin ihlal edilmiş olduğunu savunmaktadır [38].

Nitelikli halin söz konusu olması için bilişim sisteminden yararlanma için verilen bedel mutlaka para mı olmalıdır? Suçun nitelikli halinin oluşması için bilişim sisteminden yararlanma için verilen bedelin mutlaka para olması gerekmez [39]. Başka şeylerin de bedel olarak ödenmesi mümkündür; burada esas olan sisteme girilmesinin bir karşılığının bulunmasıdır.

Bir bilişim sistemindeki hizmetler ücretsiz verilip sistemde reklamlar gösterilerek sistemin sürdürülebilirliği sağlanabilir. Sistemde herhangi bir reklam dahi gösterilmeksizin sistemin bilinirliğinin artırılması ve bu şekilde, sistemin bütünsel değerinin artırılması şeklinde bir yöntem de izlenebilir. Tüm bu örnekler dışında, bedel olarak sistem kullanıcısının işlemci gücünün de kullanıldığı örnekler vardır. Özellikle kripto paraların madenciliğinde tarayıcı seviyesinde dahi çalışan uygulamalar vardır. Bu şekilde kullanıcı sisteme erişmekte, hizmetleri kullanmakta ancak bu hizmetin karşılığı olarak kendi sisteminde madencilik faaliyeti yapılmasına ve de işlemci gücünün kullanılmasına izin vermektedir.

Türk Ceza Kanunu'nun 2. maddesinde yer alan suçta ve cezada kanunilik ilkesi gereğince kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. Kanunilik ilkesinin gereği olarak suçun tüm unsurlarının belirli olması gerekmektedir. Bu doğrultuda, suçların kanunda düzenlenmesi yetmez; ayrıca bu düzenlemenin belirsiz olmaması, net ve açık olması gerekir [40]. Haklı olarak belirtildiği üzere bedeli karşılığı yararlanılabilen sistem kavramından neyin anlaşılması gerektiği açık değildir [41]. Yukarıda da açıklandığı üzere teknolojinin gelişmesiyle birlikte bilişim sistemlerinde çok farklı gelir ve işleyiş modelleri geliştirilmiştir. Bedeli karşılığı yararlanılabilen sistem durumunda ceza indiriminin yapılmasının yerindeliği de korunan hukuki değerler bakımından tartışmalıdır. Tüm bu değerlendirmeler ışığında

ve özellikle de suçta ve cezada kanunilik ilkesinin en önemli unsuru olan hukuki belirlilik açısından bilişim sistemine girme veya sistemde kalma suçunun nitelikli hali olan, Türk Ceza Kanunu'nun 243. maddesinin ikinci fıkrasında düzenlenen cezayı hafifleten halin kaldırılması amaca uygun düşecektir. Bilişim sistemleri arasında ayrım yapılması suçun muhakemesini de zorlaştırmaktadır. Bilişim suçlarıyla en etkin mücadele yöntemi, bilişim suçlarının en sade şekilde düzenlenmesi ve özel bir neden haklı kılmadıkça bir ayrım yapılmamasıdır.

e. Suçun Neticesi Sebebiyle Ağırlaştırılmış Hali

Türk Ceza Kanunu'nun 243. maddesinin üçüncü fıkrasında bilişim sistemine girme veya sistemde kalma suçunun neticesi sebebiyle ağırlaştırılmış özel hali düzenlenmiştir. Söz konusu hükme göre bilişim sistemine girme veya sistemde kalma fiilleri nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur. Verinin yok olması veya verinin değişmesi seçimlik sonuçlardır ve ağırlaştırılmış neticenin oluşması için verinin yok olması veya verinin değişmesi arasında fark yoktur [42].

Türk Ceza Kanunu'nun gerekçesinde belirtildiği üzere, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerektiği belirtilmiştir. Eğer failin verileri yok etmek veya değiştirmek kastı varsa, Türk Ceza Kanunu'nun 243. maddesinin üçüncü fıkrası değil; müstakil bir suç olan 244. maddesinin ikinci fıkrası uygulanacaktır [43]. Bu sebepledir ki 243. maddenin üçüncü fıkrasının uygulanabilmesi açısından failin ağırlaşan netice yönünden taksirinin bulunması gerekir [44].

243. maddenin ikinci fıkrasında nitelikli hal olarak düzenlenen bedeli karşılığı yararlanılabilen sistemlere yönelik bilişim sistemine girme veya sistemde kalma suçunun işlenmesi halinde ve bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, suçun neticesi sebebiyle ağırlaştırılmış hali bu durumda da uygulanacak mıdır? 243. maddenin üçüncü fıkrasının açıkça bir istisna getirmemesi sebebiyle, bedeli karşılığı yararlanılan bilişim sistemleri için de 243. maddenin üçüncü fıkrasında yer alan artırılmış cezanın uygulanması gerektiği kabul edilmektedir [45].

Türk Ceza Kanunu'nun gerekçesinde de belirtildiği üzere, sistem içindeki bütün soyut unsurlar, hükümde geçen veri teriminin kap-

samındadır. Bu doğrultuda, yanıtlanması gereken önemli bir soru da şudur: hukuka aykırı bilişim sistemine girme veya sistemde kalma suçunun netice sebebiyle ağırlaştırılmış halinin uygulanması bakımından, yok olan veya değişen verilerin önem ve niteliği bir fark oluşturacak mıdır? Yok edilen ya da değiştirilen veriler arasında önem bakımından farklılık olsa da Türk Ceza Kanunu'nda bu konuda bir ayrıma gidilmemiştir [46]. Bu bağlamda, hangi verinin, kimin aşçısından, hangi zamanda önemli olacağı ve bunun neye göre tespit edileceğinin zorluğu göz önüne alınarak, suçun cezasının üst sınırının biraz daha yukarı çekilerek hâkime takdir yetkisi tanınması önerilmektedir [47].

Adli bilişim bölümünde de değinileceği üzere bir bilişim sistemine, örneğin bir bilgisayarın işletim sistemine izinsiz girilmesi veya sistemde kalınması durumunda, işletim sisteminin kendisi farklı dosyalara çeşitli veriler girer ve işlem kayıtları tutulur. Denilebilir ki, sisteme her bir izinsiz giriş otomatik olarak sistemdeki bazı verileri değiştirir. Gerekçede belirtildiği üzere sistem içindeki bütün soyut unsurlar, 243. maddenin üçüncü fıkrasında geçen "veri" teriminin kapsamındadır. Eğer ki veriler açısından bir ayrım yapılmazsa, işletim sisteminin kullanıcı açısından önemi olmayan fonksiyonel bir dosyası veya işlem kaydının değişmesi sebebiyle doğrudan suçun neticesi sebebiyle ağırlaşmış halinin uygulanması söz konusu olacaktır. Şüphesiz bu yorum, ilgili hükmü alabildiğine genişletecek ve hukuki belirsizliğe yol açacaktır. Bu sebeple, bilişim sistemine girildiği her durumda işlem kayıtları tutulduğundan ve bu durum, verilerin değişmesine neden olduğundan, söz konusu bu veriler üzerindeki değişiklikler, "bilişim sistemine girme" fiili (birinci fıkra) kapsamında değerlendirilmelidir. Üçüncü fıkrada neticesi sebebiyle ağırlaşan hal olarak düzenlenen durum ise, söz konusu zorunlu işlem kayıtları dışındaki veriler olarak değerlendirilmelidir. Bu şekilde, amaca uygun daraltıcı yorum yapmak yerinde olacaktır.

6.2.2.3. Tipikliğin Manevi Unsuru

Türk Ceza Kanunu'nun 21. maddesinde belirtildiği üzere suçun oluşması, kastın varlığına bağlıdır. Kast, suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesidir. Öte yandan, Türk Ceza Kanunu'nun 22. maddesine göre taksirle işlenen fiiller, kanunun açıkça belirttiği hallerde cezalandırılır. Bilişim sistemine

girme veya sistemde kalma suçu ancak kasten işlenebilen bir suçtur. Dikkatsizlik veya özensizlik sebebiyle bilişim sistemine girilmesi ve bu durum fark edilir edilmez sistemden çıkılması durumunda bu suç oluşmayacaktır [48]. Suçun oluşması için ayrıca özel bir saik (amaç) aranmadığı için merak, eğlence veya oyun saiki ile hareket edilmiş olması suçun oluşmasını engellemeyecektir [49]. Uygulamada, bilgi güvenliği hizmeti veren bazı kişiler veya şirketler, potansiyel müşterilerinin sistemlerini izinsiz olarak incelemekte ve hatta bilişim sistemlerine girmektedir. Bilgi güvenliği hizmeti sağlama amacıyla da olsa, bilişim sisteminin sahibinin rızası olmaksızın bu tür bilişim sistemlerine erişim hukuka aykırıdır ve bilişim sistemine hukuka aykırı olarak girme veya sistemde kalma suçu (diğer şartların da varlığı durumunda) söz konusu olur.

6.2.2.4. Hukuka Aykırılık Unsuru

Hukuka aykırılık, en geniş tanımıyla fiilin hukukça korunmuş bir hakka veya yarara saldırı halinde olması, hukuk düzenine uygun olmaması; ceza hukuku bağlamında ise suç tipini ihlal eden hareketin, sadece ceza hukukuyla değil, tüm hukuk düzeni ile çelişki halinde bulunması olarak ifade edilebilir [50]. Türk Ceza Kanunu'nda bazı açık düzenlemelerle hukuka uygunluk sebepleri belirlenmiştir. Diğer bir deyişle, bu tür durumların varlığında fiil ile hukuk düzeni arasında çelişki yoktur.

a. Kanun Hükmünün Yerine Getirilmesi

Türk Ceza Kanunu'nun "Ceza Sorumluluğunu Kaldıran veya Azaltan Nedenler" başlıklı İkinci Bölümü altında düzenlenen 24. maddesinin birinci fıkrası uyarınca, kanunun hükmünü yerine getiren kimseye ceza verilmeyecektir. Bu doğrultuda yasal bir denetim amacıyla veya suç soruşturması kapsamında adli bilişim incelemesi yapmak amacıyla bilişim sistemine girilmesi veya orada kalmaya devam edilmesi durumlarında, bilişim sistemine girme veya sistemde kalma suçu oluşmayacaktır; yeter ki, hukuki olarak denetleme veya adli bilişim incelemesi için belirlenen sınırlar içerisinde kalınsın. Örneğin, Ceza Muhakemesi Kanunu'nun Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma madde başlıklı 134. maddesine göre yapılacak adli bilişim incelemesi hukuka uygunluk sebebi olarak kabul edilecektir. Öte yandan, Türk Ceza Kanunu'nun 24. maddesinin üçüncü fıkrası ge-

reğince, konusu suç teşkil eden emir hiçbir surette yerine getirilemez. Aksi takdirde, yerine getiren ile emri veren sorumlu olur. Bu doğrultuda, kanuni bir dayanağa dayalı olmayan bir bilişim sistemi incelemesi, amirin bu konudaki emrine rağmen, hukuki ve cezai sorumluluk doğuracaktır.

b. Meşru Savunma

Türk Ceza Kanunu'nda düzenlenen bir diğer hukuka uygunluk sebebi ise meşru savunma ve zorunluluk halidir. Türk Ceza Kanunu'nun 25. maddesinin birinci fırkasına uyarınca gerek kendisine ve gerek başkasına ait bir hakka yönelmiş, gerçekleşen, gerçekleşmesi veya tekrarı muhakkak olan haksız bir saldırıyı, o anda hal ve koşullara göre saldırı ile orantılı biçimde defetmek zorunluluğu ile işlenen fiillerden dolayı faile ceza verilmeyecektir. Bilişim sistemine girme veya sistemde kalma suçu için de meşru savunma hakkının kullanılması söz konusu olabilecek midir? Bu konuda en kritik sorulardan birisi, sisteme girilmiş ve orada kalmaya devam ediliyorsa veya Türk Ceza Kanunu'nun 244. maddesinde düzenlenen verilere zarar verilmesi hareketlerinden birisi gerçekleşiyorsa, mağdurun ya da bunun farkına varan üçüncü bir kişinin (örneğin, güvenlik altyapısını yöneten bilgi güvenliği şirketinin), failin sistemine karşı saldırı düzenlemesi ve failin kullandığı sisteme zarar vermesi durumunda haklı savunma hukuka uygunluk nedeninden faydalanıp faydalanamayacağıdır [50].

Türk Ceza Kanunu'nun 25. maddesinin birinci fıkrasında yer alan o anda hal ve koşullara göre saldırı ile orantılı biçimde defetme zorunluluğunun gerçekleştiğinden söz edebilmenin mümkün görünmediği; zira, teknik açıdan bilişim sistemine yapılan saldırının kapsamının o anda belirlenmesinin her zaman mümkün olmadığı; saldırının orantılı biçimde defedilebilmesi ve sonrasında bunun yargılama esnasında ispat edilmesinin güç olduğu; genel olarak haklı savunma halinin koşullarını ve ölçüsünü koymanın zor olduğu; yine aynı doğrultuda bu hakkın varlığından bahsedildiği aşamalarda bilişim suçlarının artacağı ve uğranılan zarara karşılık veriliyor savunmasının mazeret olarak kullanılacağı; diğer bir deyişle hukuka aykırılıkları artıracağı ve en önemlisi de bu tür bir karşı saldırı neticesinde elde edilecek delillerin de hukuka aykırı yöntemle elde edildiği için yasak delil olarak kabul edileceği ileri sürülmektedir [52].

Bilişim sistemine girme veya sistemde kalma suçunun failinin tespiti, teknik olarak kapsamlı bir adli bilişim incelemesi gerektirir. Bu çalışmanın dördüncü bölümünde etraflıca açıklanacağı üzere klasik adli bilişim incelemeleri, yeni teknolojiler karşısında yetersiz kalmaktadır. Bilindiği üzere bilişim suçlarının muhakemesindeki en zor kısım failin tespitidir. Bilişim suçu failleri, çoğu zaman anonim araçlar kullanarak veya başka kişilerin bilişim sistemlerini aracı olarak kullanarak bilişim suçlarını işlemektedir. Örneğin, saldırı anında tespit edilen ve karşı saldırı yapılacak bir IP adresinin, masum başka bir kişiye ait IP adresi olması kuvvetle muhtemeldir. Karşı bilişim sistemine girmek için yapılacak fiiller, bu bağlamda hukuka uygunluk şemsiyesi altında değerlendirilmeyecektir. İzin peşinden gidilmesi ve bilişim sistemine girilmesi, bu doğrultuda mağdurun, müstakil bir bilişim suçunun faili olması sonucunu doğuracaktır.

Bilişim sistemine yönelik saldırıyı savuşturmak için karşı bilişim sistemine girmek yerine sadece sistem engellenirse hukuka uygunluğun varlığından bahsedilebilir mi? Örneğin, belirli bir IP adresinden bilişim sistemine giriş yapıldığı tespit edilmiştir ve ancak teknik bazı imkansızlıklar sebebiyle o an sistemdeki açık kapatılamamakta veya bağlantı kısıtlanamamaktadır. Böyle bir durumda, mağdur tarafından, müstakil sistemler üzerinden tespit edilen IP adresine yönelik örneğin DDos[53]. saldırısı başlatıp veya benzeri bir teknik kullanıp söz konusu IP adresindeki bilişim sistemi işlevsiz kılınsa, bu fiil hukuka uygunluk şemsiyesi altında değerlendirilecek midir? Yukarıda belirtildiği üzere, meşru savunma kapsamında cezalandırılmamak için kişinin gerek kendisine ve gerek başkasına ait bir hakka yönelmiş, gerçekleşen, gerçekleşmesi veya tekrarı muhakkak olan haksız bir saldırı olmalı ve o anda, hal ve koşullara göre saldırı ile orantılı biçimde, defetmek zorunluluğu ile işlenen bir fiil söz konusu olmalıdır. Bu durumda gerçekleşen, gerçekleşmesi veya tekrarı muhakkak olan haksız bir saldırıdan bahsedilebilir. Karşı saldırının sadece ama sadece sistemin güvenliğinin sağlanması, veri sızıntısının durdurulması, haksız erişimin önlenmesi amaçlarıyla ve süreyle sınırlı olarak yapılması durumunda o andaki hal ve koşullara göre saldırı ile orantılı bir defetmeden söz edilebilir. Böyle bir durumda ispat külfeti, bilişim sistemine girme veya sistemde kalma suçunun mağdurunun üzerinde olacaktır ve yukarıda haklı olarak belirtildiği üzere, bu ispat çok kolay değildir. Yine de

somut olayın özelliklerine göre karşı saldırı durumunda, Türk Ceza Kanunu'nun 29. maddesinde yer alan haksız tahrik hükümlerinin değerlendirilmesi düşünülebilir.

c. Mağdurun Rızası

Türk Ceza Kanunu'nda düzenlenen diğer bir hukuka uygunluk sebebi mağdurun rızasıdır. Türk Ceza Kanunu'nun "Hakkın kullanılması ve ilgilinin rızası" başlıklı 26. maddesinin ikinci fıkrası uyarınca kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez.

Mağdurun, rızasını, suçun işlenmesinden önce ya da suçun işlendiği sırada açık veya örtülü olarak açıklamış olması gerekir [54]. Öte yandan, failin; mağdurun rızası olmaksızın sisteme girmesi ve sistemde kalmaya devam etmesi, ancak durumdan sonradan haberdar olan mağdurun bu duruma rıza göstermesi halinde de rıza, hem sisteme girişi hem de sistemde kalışı kapsayan bir hukuka uygunluk sağladığı için fiilden dolayı ceza verilmeyecektir [55].

Rıza, hukuki bir işlemdir. Hukuki işlem, hukukun kendisine sonuç bağladığı irade açıklaması demektir [56]. Hukuki netice doğurabilmesi için mağdur tarafından açıklanan rızanın, rızayı bozan nedenlerden etkilenmemiş olması gerekir; nihayetinde, rızanın ciddi olmadığını ortaya koyan latifeler, hata, hile ve ikrah gibi durumlarda rıza yok sayılır [57]. Rıza, bir hukuki işlem olduğu için, hukuken fiil tamamlanıncaya kadar geri alınabilir. Bu durumda, fiilin icrasına başlandıktan sonra rıza geri alınırsa, rıza alınıncaya kadarki tüm fiiller hukuka uygun; rızanın geri alınmasından sonra gerçekleştirilen hareketler ise hukuka aykırı kabul edilecektir [58].

Rızaya dayalı hukuka uygunluk sebebinde ispat nasıl gerçekleşecektir? Failin bir bilişim sistemine hak sahibinin haberi olmaksızın girmesi ve orada kalmaya devam etmesi halinde, söz konusu sisteme girişin ve sistemde kalmaya devam edişin rızaya dayalı olarak gerçekleşmediğini mağdurun değil, bunun rızaya dayalı olduğunu failin ispatlaması gerektiği belirtilmektedir [59].

Yukarıda da belirtildiği üzere Türk Ceza Kanunu'nun 26. maddesinin ikinci fıkrasında düzenlenen ceza sorumluluğunu kaldıran hallerden birisi olan mağdurun rızası, ancak kişinin üzerinde mutlak

surette tasarruf edebileceği bir hakka ilişkin olabilir. Dolayısıyla, kişinin üzerinde mutlak surette tasarruf edebileceği bir hak söz konusu değilse, açık veya zımni şekilde ifade edilen rızanın hukuki bir değeri yoktur. Rızayı sadece hak sahibi verebilir [60]. Bu konuda şu örnek yol göstericidir: bir bankanın personeline sisteme girebilmesi için şifre verilmesi; ancak bu personelin şifreyi bankayla ilgisi olmayan bir kişiye vermesi halinde, şifreyi alan kişinin sisteme girmesi durumunda sisteme giriş için gerekli rıza yetkili kişi tarafından verilmediğinden, personelden şifreyi alan kimsenin sisteme girmesi halinde suç oluşacaktır [61].

Mağdurun açık veya örtülü rızası durumunda suç oluşmayacaktır. Rıza konusu, özellikle sızma testleri (penetrasyon testi) gibi üçüncü kişilerin bilişim sistemine girmesi ve orada kalması açısından izin verildiği durumlarda önem taşımaktadır. Sızma testleri, sistemin zaaflarının tespiti için alınan bir hizmettir. Hizmet alınan bir şirket veya kişi, incelemeye konu bilişim sisteminin sınırlarını zorlayarak, mümkün olan her ihtimali değerlendirerek sistemin açığını bulmaya çalışır. Sızma testleri, bir akdi ilişkiye dayanır. Her bilişim sistemine göre (örneğin, uygulama, dosya sunucusu, yerel ağ, kablosuz ağ vb.) farklı kontrol alanları vardır. En basit anlatımla müşteri, hizmet sağlayıcıdan belirtilen kontrol alanlarında genel hatları tanımlanmış incelemeyi ve testleri yapmasını talep etmektedir. Rıza, bir hukuka uygunluk sebebi olarak, hizmet kapsamında kalındığı sürece, bilişim sistemine girme veya sistemde kalma suçunun oluşmasını önleyecektir. Ancak hizmet sağlayıcı, kendisine tanınan alan dışına çıktığı an artık hukuka uygunluk alanından da çıkmış olacaktır. Örneğin, açıkça uygulamaya yönelik sızma testi hizmeti talep edilen bir hizmet sağlayıcı, uygulamayla bağlantılı olmayan ve haliyle sızma testinin akdi ilişkisi dışında bir alanda inisiyatif alarak kablosuz ağ ile ilgili test yapar ve sisteme girer veya sistemde kalırsa suç oluşacaktır. Bu sebeple, bilgi güvenliği alanında hizmet verilirken hizmetin açıkça tanımlanması, hukuka uygunluğun tespiti açısından ve haliyle tarafların menfaatinin korunması için önemlidir.

Yukarıda da belirtildiği üzere sadece bilişim sistemine girme değil, bilişim sisteminde kalmaya devam etme de müstakil bir fiil olarak cezalandırılmaktadır. Mağdurun rızasını geri alması, bilişim sisteminde kalmaya devam etme suçunun müstakil şekilde oluşmasını sağlamaktadır. Örneğin, kişiye bilişim sistemine giriş izni verilmiş-

tir ancak değişen hukuki ilişki sebebiyle giriş yetkisi kaldırılmıştır. Benzer şekilde, bilişim sistemi başkası tarafından kırılmıştır ve mevcut güvenlik önlemleri kaldırılmıştır. Tüm bu ihtimallerde, bilişim sisteminde kalmaya devam edilmesi durumunda söz konusu suç oluşacaktır.

Uygulamada karşılaşılan diğer durumlar ise kendini ispat için bilişim sistemine girme ve bir meydan okumanın neticesi olarak bilişim sistemine girilmesidir. Bir kişinin, kendi teknik yeterliğini ispat için bilişim sistemine girmesi durumunda bir hukuka uygunluk sebebinden yararlanılmaz. Bu durumda suç, tüm unsurlarıyla oluşur. Dolayısıyla, herhangi bir menfaat elde edilmese de kişinin kendini ispat için bilişim sistemine girmesi durumunda suç oluşacaktır. Öte yandan, iki kişi arasında bilişim sistemine girilip girilemeyeceği konusunda bir iddialaşma olursa veya karşılıklı meydan okuma söz konusuysa ve taraflardan birisi, diğerinin hukuken erişim yetkisini haiz olduğu sisteme giriş yaparsa, iddialaşma kapsamındaki sistem için bir rızadan bahsedilebilir ve bu durumda hukuka uygunluk nedeni devreye girecektir. Ancak bu durumda önemli olan nokta, iddianın konusunun, tamamen taraflardan birisinin mutlak tasarruf yetkisini haiz olduğu bilişim sistemi olmasıdır. Örneğin, bir çalışanın başka bir kişiyle çalıştığı şirkete yönelik bir iddialaşmaya girmesi durumunda hukuki menfaatin sahibi, kişi değil şirketin kendisi olduğu için çalışanın vermiş olduğu rıza bilişim sistemine girme eylemini hukuka uygun hale getirmeyecektir. Tüm bu ihtimallerde, ayrıca iddia ve meydan okumanın kapsamına da ayrıca dikkat edilmesi gerekir. Bilişim sistemine girmeye yönelik iddianın olduğu durumda, taksirle bilişim sistemindeki veriler yok edilir veya sistemin işleyişi bozulursa, bu durumda hukuka uygunluk nedenlerinde sınırın aşılması kurallarının dikkate alınması gereklidir.

Son husus ise, bilişim sistemine güvenlik açığını kapamak amacıyla girilmesidir. İlk bölümde belirtildiği üzere, bilişim suçlularının motivasyonu çeşitlilik göstermekte ve tüm yapılan listelemeler tüketici nitelikte değildir. Gri şapkalı olarak adlandırılan hackerlar, bazen hukuka aykırı davranışlarda bulunurken, bazen ise etik standartlar çerçevesinde bazı eylemler gerçekleştirebilmektedir [62]. Örneğin, gri şapkalı hacker, açığını tespit ettiği bilişim sistemlerine girip, başkalarının bu sistemi istismar etmesini önlemek için sistemi güncelleyebilir, yama kurabilir ve açığı kapatabilir. Benzer şekilde, açığı

bilinen sisteme girip sadece basit bir uyarı yerleştirip sistem kullanıcısının sistemi güncellemesi için ikaz edebilir. Bu örneklerde amaç bilişim sistemine zarar vermek değil; tam aksine bilişim sisteminin korunmasıdır. Özel hukuk bağlamında bir nevi vekaletsiz iş görme durumuna bile benzetilecek tüm bu örnekler, ceza hukuku bağlamında hukuka uygunluk nedeni olarak kabul edilmeyecek ve bilişim sistemine giren kişinin cezai sorumluluğu söz konusu olacaktır.

ç. Hakkın Kullanılması

Türk Ceza Kanunu'nun 26. maddesinin birinci fırkası uyarınca hakkını kullanan kimseye ceza verilmeyecektir. Hakkın kullanımı bir hukuka uygunluk nedenidir ve hukuken tanınmış bir hak ya da yetkinin kullanılmasına izin veren hukuk düzeni, aynı zamanda onu yasaklayamayacağından, böyle bir durumda gerçekleştirilen fiil, hukuka uygun kabul edilir. Haklı olarak belirtildiği üzere kanun, hak veya yetkinin kullanılmasını genel bir hükümle düzenlemediğinden, her olayda durumun ayrı ayrı değerlendirilmesi gerekir [63]. Uygulamadan bir örnek vermek gerekirse; müşteri veri merkezinden yedekleme hizmeti almaktadır. Hizmet sağlayıcı müşteriye ücret karşılığında verilerini sistemlerinde yedekleme hizmeti vermektedir. Müşteri hizmet sözleşmesinde belirtilen sürede ödeme yapmadığı için hizmet sağlayıcı müşterinin sisteme erişimini kısıtlamıştır. Müşteri verilerine erişmek için hizmet sağlayıcının sistemlerine girerse bu durum hakkın kullanımı olarak değerlendirilmeyecektir. Zira, sözleşmenin ihlali sebebiyle hak kısıtlanmıştır.

d. Hukuka Aykırılık Unsuru Sorunsalı

Türk Ceza Kanunu'nun 243. maddesinde yer alan suçun oluşması için bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girilmesi veya orada kalmaya devam edilmesi gerekmektedir. Kanun, açıkça "hukuka aykırı olarak" ifadesini kullanmıştır. Esasında, ceza hukuku anlamında hukuka aykırılık, suç tipini ihlal eden hareketin sadece ceza hukukuyla değil, tüm hukuk düzeni ile çelişki halinde bulunması demektir [64]. Nitekim, hukuka aykırılık her suçta aranan, suçun temel unsurudur. Hukuka aykırılığın, bilişim sistemine girme suçunda olduğu gibi ayrıca belirtilmesinin özel bir anlamı var mıdır? Bu ifade sadece basit bir vurgu olarak mı değerlendirilmelidir; yoksa hukuki hukuki neticesi olan müstakil bir unsur olarak mı değerlendirilmelidir?

Hukuka aykırılığın kanunda ayrıca belirtildiği suç tiplerine, tam olmayan suçlar denildiği; bu suç tipleri ihlal edildiği zaman, hâkimin bu ihlalin hukuka aykırılığı da ihtiva ettiği ve hukuka aykırılığın karinesini teşkil ettiği esasından hareket edemeyeceği; hâkimin bu suçlarda hukuka aykırılığın varlığını ayrıca tespit etmesi zorunlu olduğu; zira, bu suçlarda failin kusurunun, hukuka özel aykırılığı da kapsaması zorunlu olduğu ileri sürülmektedir [65]. Genel durumlarda ise, failin hareketinden sonra, bunu yasaklayıcı bir normun olup olmadığının araştırılacağı; varlığı tespit edildikten sonra, genel hukuka aykırılık unsurunun gerçekleştiği sonucuna varılacağı belirtilmektedir. Aynı doğrultuda, açıkça "hukuka aykırılık" ifadelerinin yer aldığı suç tiplerinde "hukuka özel aykırılık" durumunun söz konusu olduğu, yasa koyucunun burada failin özellikle hukuka aykırı olarak hareket edip etmediğinin araştırılmasını ve bunun ispatlanmasını istediği, aksi takdirde, yani failin hukuka aykırı olarak hareket ettiğinin ispat edilememesi halinde cezalandırılamayacağı, suç tipinde failin eylemleri "hukuka aykırı olarak" gerçekleştirmesinin özellikle belirtilmesinin amacının bu olduğu tartışılmaktadır [66].

6.2.2.5. Suçun Özel Görünüş Halleri

a. Teşebbüs

Türk Ceza Kanunu'nun 35. maddesi uyarınca kişi, işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise teşebbüsten dolayı sorumlu tutulur. Tamamlanmış suçlar hangi sebeple cezalandırılıyorlarsa, teşebbüs aşamasında kalan suçlar da o sebeple cezalandırılırlar; çünkü her iki durumda da sosyal barış ve düzenin bozulduğu, bu sebeple teşebbüsün cezalandırıldığı kabul edilmektedir [67]. Suça teşebbüs halinde fail, meydana gelen zarar veya tehlikenin ağırlığına göre, ağırlaştırılmış müebbet hapis cezası yerine on üç yıldan yirmi yıla kadar, müebbet hapis cezası yerine dokuz yıldan on beş yıla kadar hapis cezası ile cezalandırılır. Diğer hallerde verilecek cezanın dörtte birinden dörtte üçüne kadarı indirilir.

Suça teşebbüsle bağlantılı bir diğer husus ise gönüllü vazgeçmedir. Türk Ceza Kanunu'nun 36. maddesi uyarınca fail, suçun icra hareketlerinden gönüllü vazgeçer veya kendi çabalarıyla suçun tamamlanmasını veya neticenin gerçekleşmesini önlerse, teşebbüsten

dolayı cezalandırılmaz; fakat tamam olan kısım esasen bir suç oluşturduğu takdirde, sadece o suça ait ceza ile cezalandırılır.

Bilişim sistemine girme suçu, yukarıda da belirtildiği üzere, salt hareket suçu olarak kabul edilmekte; bu bağlamda bilişim sistemine kasten ve hukuka aykırı girilmesiyle tamamlandığı için bu suçun teşebbüs aşamasında kalması zor görülmektedir [68]. Suçun teşebbüs aşamasında kalabileceği bir ihtimal olarak örneğin, girilmek istenen sistemin güvenlik yazılımları nedeniyle veya işlem sırasında elektriklerin kesilmesi yüzünden failin girme hareketini tamamlayamadığı durumlar gösterilmektedir. Esasında bu tür durumlarda sisteme girilmiş ise suç zaten oluşmuştur. Nihayetinde, suçun oluşması için belirli bir süre de olsa kalma şartı yoktur. 2016 yılındaki değişiklikle sisteme girme veya sistemde kalma müstakil olarak tipikliğin unsuru olarak tanımlanmıştır. Sisteme girilmediği bir durumda ise teşebbüsün varlığından bahsetmek zordur. Öte yandan, teşebbüs olarak nitelendirilebilecek hallerde, veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçu gibi müstakil suçların oluşup oluşmadığının ayrıca değerlendirilmesi yerinde olacaktır.

b. Suçluların Çokluğu (İştirak)

Bilişim sistemine girme veya sistemde kalma suçu, suçluların çokluğu (iştirak) bakımından bir özellik taşımamaktadır. Türk Ceza Kanunu'nda belirtilen iştirak hükümleri bu suç için uygulanabilir. Bilişim sistemine girme veya sistemde kalma suçu için iş bölümü yapılmış olabilir. Örneğin, faillerden birisi sistem hakkında bilgi toplayıp sisteme girişi planlarken, diğer bir fail güvenliğinin kırılması için uygulamayı geliştirebilir ve bunlardan bağımsız üçüncü bir fail ise uygun zamanda geliştirilen uygulamayı kullanarak bilişim sistemine girebilir. Türk Ceza Kanunu'nda düzenlenen azmettirme ve yardım etme kuralları, bilişim sistemine girme veya sistemde kalma suçu için de aynı şekilde uygulanacaktır.

c. Suçların Çokluğu (İçtima)

Suçun özel görünüş hallerinden bir diğer önemli hali içtima, suçların çokluğudur. Türk Ceza Kanunu'nun "Zincirleme suç" başlıklı 43. maddesi uyarınca bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir. Ancak bu ceza, dörtte birin-

den dörtte üçüne kadar artırılır. Aynı hükme göre bir suçun temel şekli ile daha ağır veya daha az cezayı gerektiren nitelikli şekilleri, aynı suç sayılır. Ayrıca, mağduru belli bir kişi olmayan suçlarda da bu hüküm uygulanır. Aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi durumunda da bu hüküm uygulanır. Öte yandan, Türk Ceza Kanunu'nun "Fikri içtima" madde başlıklı 44. maddesi uyarınca işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır.

Bilişim sistemine girme veya sistemde kalma suçu için de zincirleme suç mümkün müdür? Örneğin;

- Failin farklı zaman aralıklarında aynı bilişim sistemine girmesi durumunda kaç farklı suç oluşacaktır?
- Failin bilişim sistemine girmesi ancak bağlantı sebebiyle sistemden düşmesi ve tekrar bağlanması durumunda kaç farklı suç oluşacaktır?
- Bazen fail, bilişim sisteminin açığını tespit eder ve sadece açığın çalıştığını denemek için sisteme giriş-çıkış yapar. Sisteme giriş yapmak için uygun anı kollar. Bazen açığın tespiti ile sisteme giriş arasında belirli bir süre geçebilir. Bu tür durumlarda kaç farklı suç oluşacaktır?
- Fail, bir evdeki, sırasıyla, masaüstü bilgisayara, dizüstü bilgisayara ve tablete hukuka aykırı giriş sağlamıştır. Bu durumda kaç suç oluşmuştur?
- Failin amacı, bilişim sistemindeki kişisel verileri ele geçirmektir; ancak, bunu gerçekleştirmek için öncelikle bilişim sistemine girmesi gerekmektedir. Bu durumda hangi suçlar oluşacaktır?
- Fail, iki kişinin ortak kullandığı bilişim sistemine giriş yapar. Bu durumda kaç suç oluşmuştur?

Bir suç işleme kararı kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda bir cezaya hükmedilecektir. Bu doğrultuda, failin, farklı zaman aralıklarında aynı bilişim sistemine girmesi durumunda, birden fazla bilişim sistemine girme suçundan dolayı tek bir cezaya artırılarak hükmedilecektir [69]. Failin, bilişim sistemine girmesi, ancak bağlantı sebebiyle

sistemden düşmesi ve tekrar bağlanması durumunda da zincirleme suçtan bahsedilecektir. Haklı olarak belirtildiği üzere, burada temel kriter, aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla sisteme girilip girilmediğidir [70]. Nitekim, artık aynı suç işleme kararından bahsedilemeyecek kadar uzun bir aralık söz konusuysa, her bir eylem için ayrı ayrı ceza verilmesi yerinde olacaktır [71].

Bazen fail, bilişim sisteminin açığını tespit eder ve sadece açığın çalıştığını denemek için sisteme giriş-çıkış yapar. Sisteme giriş yapmak için uygun anı kollar. Bazen, açığın tespiti ile sisteme giriş arasında belirli bir süre geçebilir. Bu tür durumlarda ise tek bir suçun oluştuğunu kabul etmek yerinde olacaktır. Aynı doğrultuda failin, bir evdeki, sırasıyla, masaüstü bilgisayara, dizüstü bilgisayara ve tablete hukuka aykırı giriş sağlaması durumunda da tek bir suçun oluştuğunu kabul etmek yerinde olacaktır.

Failin amacı, bilişim sistemindeki kişisel verileri ele geçirmektir ancak bunu gerçekleştirmek için öncelikle bilişim sistemine girmesi gerekmektedir. Diğer bir deyişle, bilişim sistemine hukuka aykırı girmek veya sistemde kalmak suçu işlenmeden dosyaların ele geçirilmesi mümkün değildir. Örneğin, bilgisayardaki şahsi fotoğrafları ele geçirmek için bilgisayara izinsiz giriş yapılmıştır. Bilişim sistemine girmenin, başka suçların işlenmesinde bir araç suç fonksiyonu görmesi durumunda, hem bilişim sistemine girme hem de duruma göre Özel hayatın gizliliğini ihlal (Madde 134), Kişisel verileri hukuka aykırı olarak ele geçirme (Madde 136) veya Haberleşme gizliliğini ihlal (Madde 132) suçlarının oluştuğu; bu doğrultuda amaç suç-araç suç ilişkisin olduğu hallerde, bu suçların icra hareketleri arasında kısmen veya tamamen bir örtüşme yoksa her bir suçtan dolayı failin ayrı ayrı cezalandırılması gerektiği kabul edilmektedir [72]. Eğer ki bu şekilde bir ilişki yoksa failin ceza sorumluluğunun Türk Ceza Kanunu'nun 44. maddesinde düzenlenen ve işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişinin, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılmasını öngören fikri içtima hükümlerine göre belirlenmesi gerektiği belirtilmektedir.

Failin, iki kişinin ortak kullandığı bilişim sistemine giriş yaptığı durumda zincirleme suç hükümlerine bakmak gerekir. Yukarıda belirtildiği üzere, aynı suçun birden fazla kişiye karşı tek bir fiil-

le işlenmesi durumunda da zincirleme suç hükmü uygulanır. Bu doğrultuda tek bir suç oluştuğunu kabul etmek yerinde olacaktır. Benzer şekilde, bir kimsenin kişisel dosyasını arkadaşının bilgisayarında muhafaza ettiği ihtimalde, fail tarafından bilgisayara girilmesi ve söz konusu dosyalara ulaşılması halinde hem bilgisayarın sahibine hem de veri sahibine karşı suç işlenmiş olacak ve koşulları bulunması durumunda aynı hüküm burada da uygulanacaktır [73].

Tüm bu soruların yanıtlarının, eylemin bir kişiye karşı işlenip işlenmediğine göre ayrıca değerlendirilmesi gerekmektedir. Eğer ki eylem farklı kimselere ait bilişim sistemlerine yönelik gerçekleştirilmişse, artık mağdur sayısınca suç olduğu kabul edilmelidir [74].

6.2.2.6. Yaptırım, Soruşturma ve Kovuşturma Usulü

Türk Ceza Kanunu'nun 243. maddesinin birinci fıkrası uyarınca 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. Türk Ceza Kanunu'nun 49. Maddesinin birinci fıkrası uyarınca süreli hapis cezası, kanunda aksi belirtilmeyen hallerde bir aydan az olamaz. 50. maddenin ikinci fıkrasına göre de suç tanımında hapis cezası ile adlî para cezasının seçenek olarak öngörüldüğü hallerde, hapis cezasına hükmedilmişse; bu ceza artık adli para cezasına çevrilmez. Dolayısıyla, bilişim sistemine girme veya sistemde kalma suçunun temel hali işlendiği durumda en az bir ay hapis cezası ve en fazla bir yıla kadar hapis cezası ya da adli para cezasına hükmedilecektir. Suçun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilecektir. Bilişim sistemine girme suçu işlenmesi sebebiyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunacaktır. Türk Ceza Kanunu'nun 246. maddesinde yer alan açık düzenleme uyarınca bilişim sistemine girme veya sistemde kalma suçunun işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur. Bilişim sistemine girme veya sistemde kalma suçu, re'sen soruşturulan ve kovuşturulan bir suçtur. Suç için öngörülen yaptırım dikkate alınarak bu suçun şikayete tabi tutulmasının daha uygun olacağı ileri sürülmektedir [75]. Suçun şikayete tabi tutulması korunan hukuki değerler dikkate alındığında daha yerinde bir yaklaşımdır.

6.2.3. Veri Nakillerini Sisteme Girmeksizin Teknik Araçla İzleme Suçu

Türk Ceza Kanunu'nun 243. maddesinin dördüncü fıkrası şu şekildedir:

> *Bilişim sistemine girme*
>
> *Madde 243- (4) (Ek: 24/3/2016-6698/30 md.) 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.*

Avrupa Konseyi Siber Suç Sözleşmesi'nin 3. maddesi, taraf devletlere kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, teknik yöntemler kullanarak başka bir bilgisayar sistemi veya verilerin bulunduğu bilgisayar sistemi üzerinden veri iletimini teknik araçlarla haksız surette izleme fiilini suç olarak tanımlama yükümlülüğü getirmiştir. Sözleşmenin bu yükümlülüğünü karşılamak amacıyla, 2016 yılında Kişisel Verilerin Korunması Kanunu'nun 30. maddesinin dördüncü fıkrasıyla, Türk Ceza Kanunu'nun 243. maddesine yeni bir fıkra eklenmiş ve "Veri nakillerini teknik araçlarla izleme suçu" ihdas edilmiştir.

6.2.3.1. Korunan Hukuki Değer

Bilişim sistemine girme suçunda korunan hukuki değer olan bilişim sistemlerinin güvenliği ve güvenilirliği bu suç bakımından da korunmaktadır. Bu değerlerin yanı sıra bu suçta korunan hukuki değerin veri iletişiminin gizliliği ve mahremiyeti olduğu belirtilmektedir [76].

6.2.3.2. Tipikliğin Maddi Unsurları

a. Fail

Suçun kanuni tanımında faile ilişkin herhangi bir özellik aranmamıştır. Bu kapsamda bilişim sistemine girme suçunda genel olarak faile ilişkin yapılan açıklamalar burada da geçerlidir.

b. Mağdur

Suçun mağduru, bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakli sırasında izlenen veri üzerinde tasarruf yetkisine sahip kimsedir [77].

c. Suçun Konusu

Suçun konusu, bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında iletilen verilerdir. Suçun kanuni tanımında veri naklinin kamuya kapalı olmasına ilişkin bir belirleme yapılmamış olsa da suçun düzenleniş biçimi gereği suçun oluşması için veri naklinin kamuya kapalı olması gerekmektedir [78]. Nitekim Avrupa Konseyi Siber Suç Sözleşmesi'nde de *"bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında"* ifadesiyle bu duruma işaret edilmiştir. Örneğin, birbirlerine yakın ve belli bir bölgede (örneğin bir binada veya binanın bir katında) bulunan bilişim sistemlerini birbirine bağlayan ağ sistemi olan LAN (Local Area Network - Yerel Ağ Alanı) üzerinden gerçekleştirilen veri nakillerinin izlenmesi bu suçu oluşturacaktır. Aynı şekilde VPN iletimi, firmalar veya resmi makamlar arası veri nakilleri kamuya açık olmayan veri nakli olarak kabul edilecektir.

ç. Hareket

Veri nakillerini teknik araçlarla izleme suçunun oluşması için bilişim sistemleri arasında gerçekleşen veri nakillerinin, sisteme girilmeksizin teknik araçlarla izlenmesi gerekmektedir. Suçun kanuni tanımında izlemenin "teknik araçlarla" yapılması gerektiği belirtildiğinden, nakledilen verinin, ilgili bilişim sisteminin ekranına bakılarak çıplak gözle izlenmesi bu suçu oluşturmayacaktır [79]. Ayrıca suçun oluşabilmesi için failin bilişim sistemine girmeksizin veri naklini izlemesi gerekmektedir. Eğer bilişim sistemine girme söz konusu ise bu suç değil bilişim sistemine girme suçu söz konusu olacaktır. Suçun kanuni tanımında izlenen verinin içeriğine ulaşılması ya da bu verinin elde edilmesi aranmamıştır. İzlemek, suçun oluşumu için yeterli olduğundan, bu suç sırf hareket suçlarındandır.

6.2.3.3. Tipikliğin Manevi Unsuru

Veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçu ancak kasten işlenebilen bir suçtur. Bu kapsamda failin, bilişim sistemleri arasında gerçekleşen veri nakillerini izlediğini, bu izlemeyi teknik araçlarla gerçekleştirdiğini ve söz konusu bu durumun hukuka aykırı olduğunu bilmesi suçun oluşumu bakımından yeterlidir. Kanuni tanımda izlemenin hukuka aykırı olması gerektiği

öngörüldüğünden ve dolayısıyla failin suçu işlerken bu hususu bilmesi gerektiğinden suçun olası kastla işlenmesi mümkün değildir [80]. Suçun taksirli şekline kanunda yer verilmemiştir. Ayrıca failin suçun maddi unsurlarını bilmesi yanında herhangi bir saikle (amaçla) hareket etmesi de aranmamıştır [81].

6.2.3.4. Hukuka Aykırılık Unsuru

Veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçunun kanuni tanımında izleme fiilinin hukuka aykırı gerçekleştirilmesi gerektiği öngörülmüştür. Bu kapsamda özellikle önleme veya adli amaçlı bir tedbir olarak veri nakillerinin izlenmesi durumunda bir hukuka uygunluk nedeninin söz konusu olacağı ifade edilebilir [82]. Adli amaçlı tedbire örnek olarak 5271 sayılı Ceza Muhakemesi Kanunu'nun "Teknik araçlarla izleme" başlıklı 140. maddesi örnek verilebilir. Aynı şekilde 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun "Adli görev ve yetkiler" başlıklı ek madde 6'da belirtilen polisin sanal ortamda işlenen suçlarla ilgili olarak sanal ortamda araştırma yapması bu suç bakımından hukuka uygunluk nedeni olacaktır.

6.2.3.5. Suçun Özel Görünüş Halleri

a. Teşebbüs

Veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçunun oluşması bakımından verilerin içeriğinin öğrenilmesi, bunların bir veri taşıma cihazına veya bir başka bilişim sistemine kaydedilmesi ya da verilerin zarar görmesi öngörülmemiştir [83]. Bu sebeple suç, bir soyut tehlike suçudur [84]. Öte yandan, izleme fiili niteliği gereği belli bir süre devam etmesi gereken bir fiil olduğundan bu suç mütemadi suçlardandır. Bu nedenle failin veri naklini izlemeye başlaması ile suç tamamlanacağından bundan sonra izleme fiilinin elde olmayan nedenlerle kesilmesi durumunda failin suça teşebbüsten değil tamamlanmış suçtan dolayı sorumlu tutulması gerekir [85]. Nihayetinde bu suça teşebbüs ancak izleme fiilinin gerçekleştirilmesine kadar mümkündür.

b. Suçluların Çokluğu (İştirak)

Suça iştirak konusunda, veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçu bir özellik arz etmez. Bu suça iştirakte genel

iştirak kuralları Türk Ceza Kanunu'nun 37. maddesi uyarınca uygulanacaktır.

c. Suçların Çokluğu (İçtima)

Veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçunun zincirleme şekilde işlenmesine engel bir durum söz konusu değildir. Bu doğrultuda, failin bir suç işleme kararıyla değişik zamanlarda aynı kişinin verilerini izlemesi durumunda Türk Ceza Kanunu'nun 43. maddesinin birinci fıkrası uyarınca ceza artırılarak tek bir cezaya hükmedilecektir. Failin teknik araçlarla izlediği nakilde birden fazla kişinin verisi mevcutsa, aynı neviden fikri içtima kuralı gereğince, Türk Ceza Kanunu'nun 43. maddesinin ikinci fıkrasına göre artırılmış tek bir cezadan sorumluluk söz konusu olacaktır.

Bu suçun oluşması bakımından nakli izlenen verilerin içeriğinin öğrenilmesi ya da naklin engellenmesi aranmamıştır. Ancak veri nakli izlenirken bu neticelere sebebiyet verilmesi de mümkündür. Bu durumda tek bir fiille hem söz konusu suçun oluşumuna hem de haberleşmenin gizliliğini ihlal, kişisel verilerin ele geçirilmesi, özel hayatın gizliliğini ihlal veya haberleşmenin engellenmesi suçlarının oluşumuna da sebebiyet verilebilecektir. Bu durumda Türk Ceza Kanunu'nun 44. maddesi uyarında farklı neviden fikri içtima kuralı uygulanacak ve fail bu suçlardan cezası en ağır olanından sorumlu olacaktır [86].

6.2.4. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu

Türk Ceza Kanunu'nun 244. maddesi şu şekildedir:

> *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.

Türk Ceza Kanunu'nun 244. maddesinin birinci fıkrasına göre bir bilişim sisteminin işleyişini engelleme veya bozma, ikinci fıkrasına göre bir bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme suç olarak öngörülmüştür. Bu suç tipinin düzenlenmesiyle Türkiye Cumhuriyeti, Avrupa Konseyi Siber Suç Sözleşmesi'nin 4., 5. ve 8. maddelerine taraf olmaktan kaynaklanan yükümlülüklerini yerine getirmiş olmaktadır.

6.2.4.1. Korunan Hukuki Değer

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu ile temel korunan hukuki değer, bilişim sistemlerinin doğru bir şekilde işleyişidir [87]. Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun topluma karşı suçlar bölümünde olduğu dikkate alındığında korunan hukuki değerin toplumun menfaatleri olduğu da söylenebilir. Zira, gündelik yaşamda pek çok faaliyet bilişim alanında gerçekleştirilmekte olup; sadece gerçek kişiler değil özel ve kamu tüzel kişileri de faaliyetlerini bilişim alanına yönlendirmektedir. Bu durumda bilişim sistemine yapılan her saldırı sistem sahibini maddi anlamda zarara uğratabileceği gibi bilişim sistemlerinin güvenilirliğinin sorgulanması nedeniyle toplum menfaatlerinin de zedelenmesine yol açacaktır. Sonuç olarak bu suç ile tipiyle korunmak istenen hukuki değer hem bireysel menfaate hem de toplumsal menfaate ilişkin olduğundan karma niteliklidir.

6.2.4.2. Tipikliğin Maddi Unsurları

a. Fail

Türk Ceza Kanunu'nun 243. maddesinde yer alan bilişim sistemine girme veya sistemde kalma suçu için yapılan açıklamalar burada da geçerlidir. Kanunda bu suçun faili bakımından bir özellik belirtilmediğinden herkes fail olabilecektir.

b. Mağdur

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, mağduru bakımından da bir özellik göstermemektedir. İşleyişi en-

gellenen, bozulan, yok edilen veya değiştirilen sistem üzerinde hak sahibi kimse, suçun mağdurudur.

c. Suçun Konusu

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunda suçun konusu birinci fıkra bakımından bilişim sisteminin işleyişi iken ikinci fıkra bakımından bilişim sistemindeki veridir [88].

ç. Hareket

Türk Ceza Kanunu'nun 244. maddesinin birinci fıkrasında yaptırım altına alınan, bilişim sisteminin engellenmesi veya bozulması neticelerine neden olabilecek fiiller iken; ikinci fıkrasında yaptırım altına alınan; sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesidir.

244. maddenin birinci fıkrası bakımından engelleme ve bozma seçimlik hareketlerdir. Engelleme, sisteme müdahalede bulunularak sistemin düzgün işlemesinden elde edilecek her türlü faydanın önlenmesi ve sistemin işlevini yerine getirememesidir. Bozma ise bilişim sisteminin bir daha kendisinden beklenilen işi yapamayacak duruma getirilmesi, bilişim sistemine zarar verilmesidir [89].

244. maddenin ikinci fıkrasında ise bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek ve var olan verileri başka bir yere göndermek fiilleri seçimlik olarak öngörülmüştür. "Bilişim sistemindeki verileri bozma" seçimlik hareketinde, failin verinin içeriğine veya yapısına müdahale ederek veriyi kısmen ya da tamamen kullanılmaz hale getirmesi söz konusudur [90]. "Verilerin yok edilmesi", bilişim sisteminde bulunan verilerin geri döndürülemez şekilde silinmesi veya ortadan kaldırılmasıdır. "Verilerin değiştirilmesi", sistemde mevcut olan verinin kullanılmasını engellemeyip verinin içerdiği bilgiyi veya bu bilginin orijinalliğini ortadan kaldıracak her türlü davranışla gerçekleştirilebilir [91]. "Verilerin erişilmez kılınması", verinin içeriğine ve yapısına müdahale edilmeksizin sistem kullanıcısının bu veriye istediği şartlarda ve olağan yollarla erişiminin engellenmesidir [92]. "Sisteme veri yerleştirmek", sistem üzerinde hak sahibi bulunan kişinin rızası olmaksızın daha önce sistemde var olmayan bir verinin bilişim sistemine yerleştirilmesidir [93]. "Var

olan verileri başka yere göndermek" ise, bilişim sisteminde bulunan verilerin bilişim sistemi dışında bulunan bir başka bilişim sistemine ya da veri taşıma aracına aktarılması, kaydedilmesi ya da kopyalanmasıdır [94].

d. Nitelikli Haller

Türk Ceza Kanunu'nun 244. maddesinin üçüncü fıkrasında, sayılan fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek cezanın yarı oranında artırılması öngörülmüştür. Aynı maddenin dördüncü fıkrasında ise yine yukarıda ifade edilen fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde verilecek cezanın iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezası olacağı öngörülmüştür. Doktrinde bu fıkranın cezayı artıran nitelikli hal olduğunu ifade edenler olmakla birlikte [95]; bu fıkrayı bağımsız bir suç olarak kabul edenler de bulunmaktadır [96].

6.2.4.3. Tipikliğin Manevi Unsuru

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun manevi unsuru kasttır. Failin bilişim sisteminin işleyişini engellediğini veya bozduğunu ya da sistemdeki verileri bozduğunu, yok ettiğini, değiştirdiğini, erişilmez kıldığını, sisteme veri yerleştirdiğini, var olan verileri başka bir yere gönderdiğini bilmesi ve istemesi yeterlidir. Suçun kanuni tanımında açıkça taksirin de cezalandırılacağı belirtilmediğinden, suçun taksirle işlenmesi mümkün değildir. Ayrıca suç tipinde doğrudan kasta işaret eden herhangi bir ifade olmadığından suç olası kastla da işlenebilir.

6.2.4.4. Hukuka Aykırılık Unsuru

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu hukuka aykırılık unsuru bakımından bir özellik arz etmez. Bilişim sistemine girme veya sistemde kalma suçu için yapılan açıklamalar burada da geçerlidir.

6.2.4.5. Suçun Özel Görünüş Halleri

a. Teşebbüs

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun birinci fıkrası bakımından sistemin engellenmesi veya bozul-

ması ile suç tamamlanacağından fail icra hareketlerine başlamasına rağmen sistem engellenmemiş ya da bozulmamışsa suç teşebbüs aşamasında kalacaktır. Aynı durum maddenin ikinci fıkrasında, verilere ilişkin belirtilen fiiller bakımından da geçerlidir. Örneğin, fail mağdurun bilişim sisteminde bulunan bir veriyi kendi bilişim sistemine aktarırken, aktarma tamamlanmadan veri nakli failin elinde bulunmayan nedenlerle kesilirse sorumluluk bu suça teşebbüsten dolayı olacaktır.

b. Suçluların Çokluğu (İştirak)

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, suça iştirak açısından bir özellik arz etmez. Bu konuda genel iştirak kuralları Türk Ceza Kanunu'nun 37. maddesi uyarınca uygulanacaktır.

c. Suçların Çokluğu (İçtima)

Bilişim sistemine girme suçunda ifade edildiği üzere, 244. maddenin üçüncü fıkrası, bilişim sistemine girme suçunun, neticesi sebebiyle ağırlaşmış halini teşkil etmektedir [97]. Bu anlamda failin kastının sistemdeki verilere zarar vermek yönünde olmaması gerekir. Zira bu durumda bilişim sistemine girme suçu değil, Türk Ceza Kanunu'nun 244. maddesinde yer alan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu söz konusu olacaktır. Öte yandan Türk Ceza Kanunu'nun 43. maddesi gereğince failin bu neticeden sorumlu olması için en azından taksirle hareket etmesi gerekecektir.

6.2.5. Yasak Cihaz Veya Programlarla İlgili Suçlar

Türk Ceza Kanunu'nun 245/A maddesi şu şekildedir:

Yasak cihaz veya programlar

Madde 245/A- (Ek: 24/3/2016-6698/30 md.)

(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

Avrupa Konseyi Siber Suç Sözleşmesi'nin 6. maddesi taraf devletlere, bilgisayar yazılımları da dahil olmak üzere, bilişim sistemine girme, veri iletimine müdahale etme, sistemi engelleme ve verilere zarar verme fiillerini gerçekleştirmek amacıyla tasarlanmış veya bu amaca uygun hale getirilmiş cihazlarla, bilişim sistemine erişimi sağlayan bilgisayar şifrelerinin, erişim kodlarının veya benzeri verilerin üretimini, satışını, kullanmak amacıyla tedarik edilmesini, ithalini, dağıtımını veya başka şekilde elde edilmesini suç olarak tanımlama yükümlülüğü getirilmiştir. Bu yükümlülüğü yerine getirmek için 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesiyle Türk Ceza Kanunu'na 245/A maddesi eklenmiş ve yasak cihaz veya programlar madde başlıklı yeni bir suç ihdas edilmiştir.

6.2.5.1. Korunan Hukuki Değer

Yasak cihaz veya programların üretilmesi ve ticareti suçu ile korunan hukuki değer toplumun bilişim sistemlerine olan güvenidir. Günümüz bilişim toplumunda birçok faaliyetin bilişim sistemleri aracılığıyla yürütüldüğü göz önüne alındığında, işlenecek bilişim suçlarına hazırlık mahiyetinde olan yasak cihaz veya programların üretilmesi ve ticaretinin toplumun bu sistemlere duyduğu güveni korumak amacıyla cezai yaptırımla yasaklanması söz konusudur. Aynı doğrultuda, söz konusu cihaz veya programların bilişim sistemlerinin işleyişi üzerindeki etkisi dikkate alındığında, bu suçta korunan hukuki değerin bilişim sistemlerinin genel olarak işleyişi, güvenliği ve güvenilirliği olduğu da söylenebilir.

6.2.5.2. Tipikliğin Maddi Unsurları

a. Fail

Yasak cihaz veya programlar suçunun faili bakımından kanuni tanımında herhangi bir sınır çizilmemiştir. Bu anlamda suçun faili herkes olabilir. Öyle ki, suçun faili olmak için teknik olarak bilişim alanında uzman olmak da zorunlu değildir. Yasak cihaz veya programı imal etmeyen ve teknik olarak söz konusu cihaz veya programı hakkında uzmanlığı olmayan ancak bu cihaz veya programı ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişiler de suçun faili olarak nitelendirilecektir.

b. Mağdur

Yasak cihaz veya programlar suçu ile Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" bölümünde yer alan suçların ve bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların hazırlık hareketleri cezalandırıldığından esasen suçun işlenmesiyle herhangi bir kişinin hakkına yönelik somut bir ihlal söz konusu değildir. Dolayısıyla bu suçta mağdur, toplumu oluşturan herkestir [98].

c. Suçun Konusu

Yasak cihaz veya programlar suçunun konusu "Bilişim Alanında Suçlar" bölümünde yer alan suçların ve bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılmış veya oluşturulmuş cihaz, bilgisayar programı, şifre veya sair güvenlik kodudur [99]. Dolayısıyla söz konusu suçların işlenmesi amacıyla yapılmamış veya oluşturulmamış cihaz, bilgisayar programı, şifre veya sair güvenlik kodu üzerinde bu suç işlenemeyecektir. Örneğin, söz konusu amaçlarla üretilmemiş bir bilgisayar programının satışa arz edilmesinden sonra kötü niyetli kimseler tarafından bu programın manipüle edilerek maddede sayılan suçların işlenmesi bakımından kullanılması durumunda satışa arz edenin Türk Ceza Kanunu'nun 245/A maddesinden sorumluluğu söz konusu olmayacaktır.

ç. Hareket

Yasak cihaz veya programlar suçu, seçimlik hareketli bir suç olarak düzenlenmiştir. Buna göre, maddede sayılan suçların işlenmesi amacıyla yapılmış cihaz, bilgisayar programı, şifre veya sair güvenlik kodunu imal etme, sevk etme, nakletme, depolama, kabul etme, satma, satışa arz etme, satın alma, başkalarına verme veya bulundurma bu suçun hareket unsurunu oluşturmaktadır. Bu seçimlik hareketlerden; kabul etme, satma, başkalarına verme hareketleri ancak çok failli olarak işlenebilir. Bu durumda söz konusu hareketleri gerçekleştiren herkes suçun faili olacaktır.

6.2.5.3. Tipikliğin Manevi Unsuru

Yasak cihaz veya programlar suçu ancak kasten işlenebilir. Suçun taksirli şekli kanunda düzenlenmemiştir. Ayrıca bu suçla esasen

maddede belirtilen suçların hazırlık hareketleri cezalandırıldığından, kanun koyucu suçun oluşumu bakımından taksiri yeterli görmemiştir. Cezai sorumluluk bakımından failin ayrıca bilişim alanında suçlar bölümünde yer alan suçların veya bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesinde kullanmak maksadıyla hareket etmesi gerekmektedir [100]. Failde; imal etme, sevk etme, nakletme, depolama, kabul etme, satma, satışa arz etme, satın alma, başkalarına verme veya bulundurma seçimlik hareketlerine ilişkin kast belirlenebiliyor ancak fail maddede sayılan suçların işlenmesi maksadıyla hareket etmiyorsa suç oluşmayacaktır. Örneğin kişi maddede sayılan suçlarda kullanılabilecek bir programı sırf merakını gidermek amacıyla ya da bir bilişim sisteminin açıklarını tespitte kullanmak amacıyla kendinde bulunduruyorsa veya bilgi güvenliği alanında koruma ve önleme amaçlı bir hizmet sunuluyorsa, Türk Ceza Kanunu'nun 245/A maddesinden sorumluluk söz konusu olmayacaktır. Aynı doğrultuda, uygulamalara içeriklerine bakmaksızın 5651 sayılı Kanundaki tanımıyla yer sağlayıcı sıfatıyla barındırma hizmeti sunan bir hizmet sağlayıcı suç işleme maksadıyla hareket etmiyorsa nakletme, depolama veya bulundurma eylemlerinden dolayı sorumlu olmayacaktır. Son olarak, tipikliğin manevi unsuru bakımından kastın yanı sıra failin belli bir maksatla hareket etmesi de arandığından bu suçun olası kastla işlenmesi mümkün değildir.

6.2.5.4. Hukuka Aykırılık Unsuru

Yasak cihaz veya programlar suçunda mağdur, toplumu oluşturan herkes olduğundan, ilgilinin rızası ve meşru savunmanın bu suç bakımından bir hukuka uygunluk nedeni olarak kabul edilmesi mümkün değildir [101]. Ancak görevin ifası ve hakkın kullanılması, bu suç bakımından geçerli olabilecek hukuka uygunluk nedenleridir. Örneğin 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesindeki şartların gerçekleşmesi durumunda bir suç dolayısıyla yapılan soruşturmada bilgisayarlara, bilgisayar programlarına ve kütüklerine kolluk tarafından el konulması ve şifrenin belirli araçlarla kırılması Türk Ceza Kanunu'nun 245/A maddesi bakımından görevin ifası kapsamında değerlendirilecek ve cezai sorumluluk söz konusu olmayacaktır. Aynı doğrultuda, bilgi güvenliği alanında faaliyet gösteren şirketlerin, zararlı yazılımları tespit etmek, analiz etmek, bunlara yönelik önlemler almak alanında vermiş olduğu hizmetler-

de maddede sayılan suç işleme maksadı olmadığı için Türk Ceza Kanunu'nun 245/A maddesi kapsamındaki suç oluşmayacaktır. Tabii ki, her somut olayın koşullarının değerlendirilmesi ve nedensellik bağının özel olarak irdelenmesi gerekir.

6.2.5.5. Suçun Özel Görünüş Halleri

a. Teşebbüs

Yasak cihaz veya programlar suçunun oluşması için kanuni tanımda ayrıca neticeye yer verilmemiştir. Suç, maddede sayılan seçimlik hareketlerden birinin yapılması ile işlenmiş olacaktır. Dolayısıyla bu suça teşebbüs kural olarak mümkün olmamakla birlikte eğer hareket kısımlara ayrılabiliyorsa teşebbüs söz konusu olacaktır. Ancak belirtmek gerekir ki bu suç bakımından sırf bulundurmanın dahi suçun seçimlik hareketlerinden sayılması, teşebbüsün gerçekleşmesini zorlaştırmaktadır. Örneğin, maddede sayılan suçların işlenmesi için elde bulundurulan bir cihazın satışını ihbar alan kolluğun satış gerçekleştirileceği sırada baskın yapması durumunda satıcı söz konusu cihazı zaten elinde bulundurduğundan suç tamamlanmış olacaktır. Ancak cihazı satın alma seçimlik hareketi henüz gerçekleşmediğinden satın alacak kişi bakımından teşebbüsün gerçekleşmiş olacağı ifade edilebilir.

b. Suçluların Çokluğu (İştirak)

Yasak cihaz veya programlar suçu, iştirak bakımından özellik arz etmez. Ancak ifade etmek gerekir ki, maddede sayılan ithal etme, kabul etme, satma, satın alma başkalarına verme seçimlik hareketleri ancak çok faille işlenebileceğinden, ilişkinin her iki tarafı da şerik olarak değil fail olarak sorumlu olacaklardır.

c. Suçların Çokluğu (İçtima)

Yasak cihaz veya programlar suçunun kanuni tanımında belirtilen hareketler seçimlik olduğundan bunlardan birden fazlasının gerçekleştirilmesi durumunda birden fazla suç oluşmayacaktır. Ancak bu durum temel cezanın belirlenmesinde hâkim tarafından göz önünde bulundurulmalıdır. Bu suç, esas olarak "Bilişim Alanında Suçlar" bölümünde yer alan suçların ve bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların hazırlık hareketlerinin cezalandırıldığı bir suçtur. Dolayısıyla Türk Ceza

Kanunu'nun 245/A maddesinde düzenlenen bu suçu işledikten sonra bilişim suçları bölümünde sayılan diğer suçlar da gerçekleştirilirse fail hakkında iki suç bakımından ayrı ayrı cezaya hükmedilecektir.

Son olarak belirtmek gerekir ki 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 72. maddesinde düzenlenen suç, Türk Ceza Kanunu'nun 245/A maddesine göre özel hüküm niteliğindedir [102]. Zira Fikir ve Sanat Eserleri Kanununda Türk Ceza Kanunu'na göre daha özel bir amaç belirlenmiştir. Söz konusu hükme göre "*Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik*" olarak program veya teknik donanımların üretilmesi, satışa arz edilmesi veya elde bulundurulması söz konusu ise hem Türk Ceza Kanunu madde 245/A hem de Fikir ve Sanat Eserleri Kanunu madde 72 bakımından tipiklik gerçekleşmiş olmakla birlikte sorumluluk Fikir ve Sanat Eserleri kanunu madde 72'den dolayı olacaktır.

6.2.6. Tüzel Kişiler Hakkında Güvenlik Tedbirleri

Türk Ceza Kanunu'nun 246. maddesi uyarınca "Bilişim Suçları" bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur. Bu doğrultuda, bir tüzel kişiliğin faaliyet izni iptal edilebileceği gibi, tüzel kişiliği hakkında müsadere kararı da verilmesi mümkündür.

6.2.7. Terörle Mücadele Kanunu

3713 sayılı Terörle Mücadele Kanunu'nun 1. maddesi terörü şu şekilde tanımlamaktadır: "*Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir*". Aynı Kanunun 2. maddesine göre ise bu belirlenen amaçlara ulaşmak için meydana getirilmiş örgütlerin mensubu olup da bu amaçlar doğrultusunda

diğerleri ile beraber veya tek başına suç işleyen veya amaçlanan suçu işlemese dahi örgütlerin mensubu olan kişi terör suçlusudur. Terör örgütüne mensup olmasa dahi örgüt adına suç işleyenler de terör suçlusu sayılır.

Terörle Mücadele Kanunu'nun "Terör amacı ile işlenen suçlar" başlıklı 4. maddesi Türk Ceza Kanunu'nun 243. maddesinde yer alan "Bilişim sistemine girme" suçu ile 244. maddesinde yer alan "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçlarının yukarıda belirtilen terör tanımına giren amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde terör suçu sayılacağını belirtmiştir.

Bir suçun terör suçu olarak kabul edilmesinin en önemli neticesi verilecek cezanın artırılmasıdır. Terörle Mücadele Kanunu'nun 5. maddesine uyarınca terör suçu olarak belirlenen suçları işleyenler hakkında ilgili kanunlara göre tayin edilecek hapis cezaları veya adli para cezaları yarı oranında artırılarak hükmolunur. Ayrıca, bu suretle tayin olunacak cezalarda, gerek o fiil için gerek her nevi ceza için belirli olan cezanın yukarı sınırı aşılabilir. Ancak, müebbet hapis cezası yerine ağırlaştırılmış müebbet hapis cezasına hükmolunur. Suçun, örgütün faaliyeti çerçevesinde işlenmiş olması dolayısıyla ilgili maddesinde cezasının artırılması öngörülmüşse; sadece bu Terörle Mücadele Kanunu'nun 5. maddesi hükmüne göre cezada artırım yapılır. Ancak, yapılacak artırım cezanın üçte ikisinden az olamaz.

6.3. Siber Güvenlik: Politika, Strateji ve Hukuk

Türkiye'de siber güvenlik alanındaki çalışmalar ve yasal düzenlemeler son yıllarda hız kazanmıştır. 2012/3842 sayılı Bakanlar Kurulu Kararı ile 11/6/2012 tarihinde Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar'ın yürürlüğe konulması kararlaştırılmış ve bu kararla Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik ile ilgili politika belirleme ve eylem planları hazırlama yetkisi verilmiştir [103].

2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı uyarınca o dönemki Telekomünikasyon İletişim Başkanlığı [104] tarafından siber güvenlik ile ilgili tehdit ve alınacak önlemlere ilişkin ulusal ve uluslararası çalışmalar yapmak için Ulusal Siber Olaylara Müdaha-

le Merkezi (USOM, TR-CERT) kurulmuştur. Bu merkez; Türkiye'de siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerinin zayıflatılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve ilgili aktörlerle paylaşılması, ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditler ile ilgili kendisine ulaştırılan ihbarları da değerlendirerek, söz konusu tehditlerin tespit ve bertaraf edilmesi amacıyla kamu kurumları, kuruluşlar ve özel kişiler ile koordinasyonun sağlanması için 7/24 esasına göre görev yapmaktadır. 2013 yılında ayrıca Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, Resmi Gazete'de yayımlanarak yürürlüğe girmiş ve kapsamında Kurumsal SOME'ler (Siber Olaylara Müdahale Ekipleri) ve sektörel SOME'ler kurulması kararlaştırılmıştır [105]. Belirtmek gerekir ki, Türkiye'de siber güvenliğin sağlanması amacıyla en temel ve güncel belge 2016-2019 Ulusal Siber Güvenlik Stratejisi'dir [106].

Yasal düzlemde ise 2014 yılında 5809 sayılı Elektronik Haberleşme Kanunu'na 6 Şubat 2014 tarih ve 6518 sayılı Kanun'un 106. maddesiyle eklenen Ek Madde 1 siber güvenlik açısından önemli bir reform niteliğindedir. Elektronik Haberleşme Kanunu'na eklenen Ek Madde 1 uyarınca kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur ve bu Kurula (a) siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları alma; (b) kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlama; (c) siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirleme görevleri verilmiştir.

Aynı değişiklik paketiyle Elektronik Haberleşme Kanunu'nun 5. maddesinin birinci bendine eklenen (h) bendiyle eski adıyla Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirleme, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirleme, eylem planlarını hazırlama, Siber Güvenlik Kurulu'nun sekretaryasını yapma, ilgili faaliyetlerin koordinasyonunu sağlama, kritik altyapılar ile ait oldukları kurumları ve konumları belirleme, gerekli müdahale merkezlerini kurma, kurdurma ve denetleme, her türlü siber müdahale

aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapma, yaptırma ve bunları teşvik etme ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütme, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlama görevi verilmiştir.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu'nun "İdari yapı ve görevler" başlıklı 10. maddesi Bilgi Teknolojileri ve İletişim Kurumu'na ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlama, gerekli tedbirlerin aldırılması konusunda faaliyet yürütme ve ihtiyaç duyulan çalışmaları yapma yetkisi tanımaktadır. 2016 yılında 671 sayılı Kanun Hükmünde Kararname'nin 25. maddesiyle Elektronik Haberleşme Kanunu'nun 60. maddesine onuncu fıkra eklenmiş ve Bilgi Teknolojileri ve İletişim Kurumu'na, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma veya aldırma yetkisi tanınmıştır. Aynı hükme eklenen on ikinci fıkrayla Bilgi Teknolojileri ve İletişim Kurumu'nun bu alandaki talimatlarına aykırılık yaptırıma bağlanmıştır.

Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği'nde 2018 yılında yapılan değişiklikle yönetmeliğin 19. madde başlığı "Şebeke ve bilgi güvenliği ile siber güvenliğe ilişkin ihlaller" olarak değiştirilmiş ve aynı maddeye şu hüküm eklenmiştir:

> *"Ulusal siber güvenlik faaliyetleri ile siber saldırılara karşı korunma ve caydırıcılığın sağlanmasına yönelik Kurumun görevleri kapsamında belirleyeceği yükümlülükleri yerine getirmeyen veya aldıracağı tedbirleri uygulamayan gerçek kişiler ile işletmeciler dışındaki özel hukuk tüzel kişilerine bin liradan bir milyon liraya kadar idarî para cezası uygulanır. Kurum ihlal konusuna ilişkin olarak gerçek veya tüzel kişiden yazılı açıklamalarını 15 günden 30 güne kadar belirlenebilecek süre içerisinde göndermesini ister. Süresinde gönderilmeyen yazılı açıklama dikkate alınmaz."*

Elektronik Haberleşme Kanunu'nun 60. maddesinin onuncu fıkrası ve Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği'nde yer alan hükümler Türk hukukunda siber güvenliğin en güçlü normatif dayanaklarıdır. Bu hükümler sadece kamu kurum ve kuruluşlarına değil, özel hukuk kişilerine de siber güvenlikle ilgili yükümlülükler yüklenmesine ve bunların ihlali durumunda yaptırım uygulanmasına dayanak oluşturmuştur. Her ne kadar hükümlerin içeriği çok geniş biçimde kaleme alınmış olsa da Türkiye'de siber güvenliğin açık yasal dayanağını oluşturmaları açısından önemlidir. Bu hükümler gereğince ve de ölçülü şekilde uygulandığı takdirde siber güvenlikle ilgili müstakil bir Siber Güvenlik Yasası yürürlüğe koyuluncaya kadar önemli bir boşluğu dolduracaktır.

6.4. Adli Bilişim

Teknolojinin gelişmesiyle veri kaydetme alışkanlıkları, verinin kaydedildiği mecralar ve bunlara erişme yöntem ve teknikleri de esaslı ölçüde değişmiştir. Dijital ortamlar asıl, kağıt ve benzeri ortamlar is istisna halini almıştır. Klasik kayıt yöntemlerin gün geçtikçe azaldığı, mobil aygıtların ve bulut teknolojilerinin artmasıyla verinin akışkanlığının arttığı bir ortamda, delillerin türü, niteliği, boyutu, nerede bulunacağı gibi hususlar da haliyle köklü bir değişikliğe uğramıştır. Ayrıca işletim sistemleri ve yazılımlardaki hızlı değişimle, dosya kayıt yöntemleri ve dosya türleri de hızlıca değişmektedir. Geliştiricilerin çeşitlenmesiyle, bazı durumlarda standart tipolojisi bile olmayan kendine özgü veya tamamen tutarsız sistemler ve dosya türleri ortaya çıkmaya başlamıştır.

Adli bilişim, bilgisayarlar veya dijital saklama aygıtlarında veya elektronik ortamda bulunan yasal delillerin elde edilmesine ilişkin olan adli bilimler altında sınıflandıran bir branştır. Bu bilim dalı uluslararası standartlarla şekillenmiştir. ISO tarafından 2012 yılında yayımlanan ve 2018 yılında gözden geçirilen ISO/IEC 27037:2012 bu alandaki en temel belgedir [107]. Bu standart, delil niteliği olabilecek dijital verilerin tanımlama, toplama ve muhafazası için yol göstermektedir. Esasında farklı ülkelerde, farklı kurumlar, kolluk kuvvetleri ve enstitülerde dijital delillerin elde edilmesi için farklı yöntem ve teknikler kullanılmaktadır. Peki, adli bilişim alanında neden bir standardizasyona ihtiyaç vardır? Bu alanda bir standardizasyona gidilmesiyle uluslararası benzer uygulamaların gelişeceği,

farklı ülkelerde farklı kişi veya kurumlarda bu tür soruşturmalar yürütüldüğü durumlarda kıyas yapmanın, karşılaştırmanın ve birleştirmenin kolaylaşacağı düşünülmektedir [108].

İlk bölüm altında da etraflıca açıklandığı üzere, bilişim suçlarını diğer suçlardan ayıran en temel özelliklerden birisi bu suçların sınır-aşan niteliğidir. Bilişim suçları, soruşturması ve kovuşturması için uluslararası adli yardımlaşma gerektiren, farklı ülkelerdeki kolluk kuvvetlerinin ve adli makamların işbirliğinin ve bilgi ve belge paylaşımının yoğun olduğu suçlardır. Deliller, toplandıkları ülke dışındaki makamların önüne sunulmaktadır. ISO standartları bu bağlamda delillerin standart şekilde farklı ülkelerdeki adli makamlar tarafından pratik şekilde kullanılmasına ve en önemlisi de dijital delillerin hukuka uygunluk denetimlerinin daha kolay şekilde yapılmasına hizmet etmektedir.

ISO/IEC 27037 dışında adli bilişimi ilgilendiren başka ISO standartları da vardır. Şöyle ki, ISO/IEC 27041:2015 [109]. standardı soruşturmalarda uygun yöntem ve araçların kullanılması konusunda yol göstermekte; ISO/IEC 27042:2015 [110] dijital delilin analizi ve yorumlanması konusunda yol göstermekte; ISO/IEC 27043:2015 [111] ise daha geniş bir perspektifle soruşturmalarda vaka incelemesine ilişkin hususlarda prensipler ortaya koymaktadır. Son olarak, ISO/IEC 27050:2016 [112] dört ayrı bölüm altında elektronik keşifle ilgili standartları belirlemektedir.

6.4.1. Adli Bilişimin Temel Safhaları

Adli bilişim incelemesinin temeli, dijital delillerin herhangi bir değişiklik yapılmaksızın toplanması ve muhakeme tamamlanıncaya kadar bütünlüklerinin temin edilmesidir [113]. Dijital delillerin en önemli sorunu hassas olmaları; yanlış bir işlem veya yanlış bir inceleme sonucunda kolayca değiştirilebilir, tahrif edilebilir, tahrip edilebilir, yok edilebilir olmalarıdır [114]. Dijital delillerin bir diğer temel özelliği ise gizli yapılarıdır [115]. Öyle ki, dijital deliler ilk bakışta gözle görülemeyen delillerdir. Bu delilleri görülebilir hale getirmek için bazı araçlara ve yazılım programlarına ihtiyaç vardır.

Dijital deliller sadece ceza davalarında değil, en sıradan davalarda, özel hukukun her alanında dava neticesini belirleyen niteliktedir. Adli bilişim dijital materyalin salt kopyasını veya imajını alma

süreci değildir. Şüphesiz imaj alma adli bilişimin önemli bir unsuruysa da, adli bilişim bunu aşan kapsamlı bir süreçtir. Adli bilişim incelemelerinde olay yerinden soruşturmacıya ve oradan da mahkemeye kadar uzanan yolda titiz bir şekilde "muhafaza zincirine" uyulması gerekir. Güvenlik güçleri tarafından, sonradan mahkeme sürecinde delil olarak kullanılacak bilgisayar veya depolama aygıtları üzerindeki verileri değiştirebilecek nitelikte hiçbir hareket yapılmamalıdır. Bilgisayar veya depolama aygıtları üzerinde bulunan orijinal veriye erişilmesinin gerekli olduğu istisnai durumlarda, bu kişinin erişime yetkili olması ve hareketinin sebep ve sonuçlarını açıklayacak deliller sunabilecek durumda olması gereklidir. Elektronik delillere uygulanan tüm süreçlerin kaydedilmesi veya işlem geçmişi raporunun (audit trail) oluşturulması ve saklanması gerekir. Bağımsız bir üçüncü tarafın izlenen süreci test etmesi ve aynı sonuçlara ulaşabilmesi gerekir.

Yukarıda belirtildiği üzere dijital deliller hassastır; yanlış bir işlem veya yanlış bir inceleme sonucunda kolayca değiştirilebilir, tahrif, tahrip veya yok edilebilirler. Bu değişiklikler yanlış yöntemin kullanılması sebebiyle ihmal suretiyle olabileceği gibi kasten de yapılabilir. Modern adli bilişimin en kritik aşaması delil kaynaklarının yerini saptamaktır [116]. Dijital delilin ilk toplandığı aşamadan itibaren muhafazasını sağlamak ve bu süreci doğrulamak amacıyla kriptografik hash değerinin alınması ve bu değerin saklanması gerekir. Bu saklama sürecinde hem elektronik muhafaza ilkelerine hem de fiziksel saklama ilkelerine uymak gerekir. Bu doğrultuda, elektronik veya manyetik aygıtlar için ısıya, rutubete, fiziksel şoklara, statik elektriğe ve manyetik kaynaklara, sıcak, nem veya soğuğa karşı gerekli önlemlerin alınması gerekir. Olay mahallinin ve olay mahallindeki tüm kişilerin güvenliği sağlandıktan sonra ilk sorumlunun klasik ve elektronik her iki türdeki delilleri görsel olarak teşhis etmesi ve çabuk kaybolacak deliller mevcutsa bunları tespit etmesi gereklidir. Ayrıca, fiziki ortamın dikkatle incelenmesi ve belgelenmesi gerekir.

Delil teşkil eden orijinal araçların tam bir çoğaltımının yapılması süreci imaj çıkartma veya görüntüleme ya da ayna görüntü alınması gibi kavramlarla ifade edilmektedir. Alınan imaj kriptografik hash ile imzalanmak suretiyle delil bütünlüğü sağlanmakta; bir nevi delil mühürlenmektedir. Delilin manipüle edilmediği matematiksel al-

goritmalar ile ispat edilir. Bu sebepledir ki, dijital delil içeren bir aygıtın imajı alınırken, şüpheli olan aygıt üzerine herhangi bir veri eklenmediğini garanti etmek için yazma koruma araçları kullanılmalıdır. İmaj almanın amacı aynı sistemi başka bir ortamda simüle edebilmektir. İmaj alma disk yüzeyini kesim (sector by sector) çoğaltır ve böylece hedef sürücünün bir ayna görüntüsünü alır. Elektronik veriler kâğıttan farklı olarak zengin gizli bilgileri örneğin, yardımcı verileri ihtiva etmektedir (metadata), bu gizli bilgiler elektronik belgenin içerisine belgeyi oluşturmak için kullanılan yazılım programı tarafından gömüldüğü için, çoğu kez ilişik (gömülü, (embedded)) veya "yardımcı veri" olarak adlandırılmaktadır [117]. Birebir imaj almak suretiyle meta-datası silinmiş olarak gözüken bir dosyanın disk yüzeyinden kurtarılması mümkündür.

Adli bilişimin delil toplama aşamasında delil içerebileceği düşünülen bilgisayarlardan uçucu deliller ve imajlar alınır; inceleme ve analiz aşamasında, imajlar üzerinden çeşitli araçlar kullanılarak ve elle incelemeler yapılır, iddiaları destekleyen veya çürüten deliller bulunur; raporlama aşamasında ise delillerin elde ediliş metotları ve kullanılan araçlar detaylarıyla açıklanır. Tüm adımların birbirini doğru sırayla takip etmesi ve muhafaza zincirine uyulması gerekir. Aynı doğrultuda materyal toplama aşamasındaki envanter ile analiz aşamasındaki envanter birbirini tutmalıdır. Aksi halde yanlış müdahale, kaza veya kasten delilin yok edilmesi ve duruma göre hukuki, cezai ve idari sorumluluğun doğması söz konusu olacaktır. Bu süreç soğuk hava zinciriyle gıda taşınmasına benzetilebilir. Zincirin bir aşamasında soğutmada sorun yaşanırsa, diğer aşamalarda soğuk hava zincirinin muhafaza edilmesini artık önemsiz kılar. Nihayetinde, gıda bozulmuştur. Adli bilişimde muhafaza zincirine uyulmaması da delili hukuka aykırı delil haline getirir. Zehirli ağacın meyvesi de zehirli olacağından, bu delilin hukuki bir etkisi kalmaz.

6.4.2. Adli Bilişim İncelemelerinde Güncel Sorunlar

Adli bilişim incelemesi kapalı bir aygıtta yapılabileceği gibi, çalışan bir aygıtta da yapılabilir. Ölü ve canlı analiz olarak anılan bu analiz türlerinde, kullanılacak yöntem ve teknikler birbirlerinden esaslı olarak farklıdır. Ölü analizde aygıta, koruma yazmalı cihazlarla müdahale edilmekte; verilerin imajı alınmakta ve kriptografik hash

ile imzalanarak dosya bütünlüğü temin edilmektedir. Ancak, bazı durumlarda çalışan bir sisteme müdahale edilmesi gereği duyulmaktadır. Örneğin, sistemde şifreli bir alan vardır ve önbellekte yer alan anahtarın kaybolmadan ele geçirilmesi gerekmektedir. Benzer şekilde sadece önbellekte çalışan bir zararlının tespiti için de canlı analiz yapılması gerekmektedir. Aynı doğrultuda, bir sistemin aktif ağ yapısı ve bağlantıları da en doğru canlı analiz ile mümkündür. Canlı analiz yapılması durumunda kullanılacak adli bilişim uygulamasının sistemde inceleme yapılması sırasında minimum da olsa sisteme veri yazma riski gibi çeşitli riskleri bulunmaktadır.

Adli bilişim alanında en güncel sorunlardan birisi akıllı telefonların adli bilişim incelemesini konu alan "mobil forensic" alanındadır. Mobil cihazların çeşitlenmesiyle beraber bu tür cihazlarda adli bilişim yapılması karmaşık hale gelmiştir. Öyle ki, bazı cihazlarda salt imajının alınması için bile root yapma gibi cihaza veri kaydedilmesi sonucu doğuracak işlemlerin yapılması gerekli olabilmektedir. Yukarıda açıklandığı üzere, adli bilişim incelemesinin en temel ilkesi inceleme yapılacak ortama yazma korumalı cihazlarla müdahale ederek hiçbir veri kaydı yapmaksızın birebir, sektör-sektör ortamın kopyasının alınmasıdır. Tutarlı tipolojisi olmayan mobil cihazlardaki inceleme bu bağlamda adli bilişimde güncel bir sorundur.

Adli bilişim açısından en güncel bir diğer sorun ise yeni teknolojilerdir. Nesnelerin İnterneti ("internet of things") olarak adlandırılan yeni teknolojilerle internete bağlı olan nesneler, cihazlar, aygıtların doğrudan internet ortamında veri paylaşımı yapması mümkün olmuştur. Bu tür nesneler evlerde, işyerlerinde, sağlık alanında, spor alanında, enerji alanında birçok farklı amaç için kullanılmaktadır. Bu tür nesneler farklı nitelikte ve mahiyette veriler içerdiği için bir suç soruşturması sırasında dijital delil olarak kullanılması söz konusu olabilir. Örneğin, akıllı bileklikteki veriler incelenerek kişinin hareketleri, konumu, kalp atış istatistikleri, uyku aşamaları, kişinin uyanık olup olmadığı, hareket edip etmediğine ilişkin bilgiler derlenebilir ve bir suç soruşturması veya kovuşturması sırasında bu tür veriler delil olarak kullanılabilir [118]. Benzer şekilde, akıllı ev aletlerinde yer alan veriler, somut olayda kişinin evde olup olmadığı veya ne yaptığı konusunda yol gösterici olabilir. Özellikle akıllı araçlardaki veriler trafikte işlenen suçların aydınlatılmasına ilişkin

kritik veriler içerdiği için araç incelemeleri müstakil bir adli bilişim alanı olarak gelişmektedir.

Her ne kadar Nesnelerin İnternetinde, aygıtlar, aletler veya cihazlar çeşitli dijital deliller içeriyorsa da adli bilişim incelemesi diğer adli bilişim incelemelerinden esaslı farklılıklar ve zorluklar içermektedir [119]. Bu zorluklar adli bilişimin her bir aşaması için farklı niteliktedir. Delil toplanması gereken cihaz sayısı fazlalaşmakta, toplanan verilerin farklı formatlarda olması inceleme sürecine geçişi zorlaştırmaktadır. IoT cihazlar arasında genel kabul görmüş kayıt (log) tutma standardı olmadığı ve de veri boyutu büyüdüğü için klasik yöntemlerle inceleme zorlaşmaktadır. İncelenen sistemler karmaşıklaştıkça raporlar daha fazla teknik detay içermekte ve dijital delili anlamlandırmak güçleşmektedir. Aynı sorunların kendine özgü sistemler için de geçerli olduğu söylenebilir. Örneğin, Raspberry Pi gibi tek devre sistemler üzerinde adli bilişim incelemesi yapmak bile artık belirli uzmanlık gerektirmekte ve kendine özgü sorunlar ortaya çıkarmaktadır [120].

Adli bilişim alanında önemli bir diğer sorun ise bulutta incelemedir. Bulut bilişimin hizmet olarak yazılım, hizmet olarak platform veya hizmet olarak altyapı şeklinde kullanıldığı ihtimallerde dijital delil bulut altyapısında yer almaktadır. İnce istemci (thin client) yerine sıfır işlemci (zero client) kullanıldığı durumlarda neredeyse yerel istemcide hiçbir veri kaydedilmemektedir. Bu tür durumlarda adli bilişim incelemesi yapılarak dijital delilin tespiti için bulutta adli bilişim incelemesi yapılması gerekmektedir. Ancak bulut bilişimde henüz standartların tam manasıyla oturmamış olması, bu alandaki altyapılar arasındaki esaslı farklılıklar sebebiyle adli bilişim incelemesi yapılması klasik adli bilişim incelemelerine göre karmaşık ve zordur [121].

Bulut bilişimde inceleme yapabilmek için öncelikle sistem erişim bilgilerinin biliniyor olması gerekir. Sisteminde inceleme yapılacak şüpheliyi bu şifreyi vermeye zorlamak hukuken çeşitli sorunlar barındırmaktadır. Türk Anayasası'nın "Suç ve cezalara ilişkin esaslar" başlıklı 38. maddesinin beşinci fıkrası uyarınca hiç kimse kendisini suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaz. Aynı doğrultuda, bulut bilişimde önemli bir sorunlu alan ise sınır aşan incelemelerdir. Bulut bilişimin yapısı gereği veriler çok farklı ülkelerde barındırılmaktadır. Bu sistemlere giriş için

şifrelerin kırılması, sistemde inceleme yapılması, veri indirilmesinin hukuka uygunluğu için verinin barındırıldığı her bir ülke hukuku açısından ayrı ayrı değerlendirme yapılması gerekmektedir [122].

Öte yandan, veri kaydetme araçlarına yönelik bilimsel araştırmaların neticesinde devrim niteliğinde bazı gelişmeler yaşanmıştır. Bunlar arasında belki de en önemlisi DNA sarmalının yeniden sentezlenmesi suretiyle 739 KB'lik verinin yazıldığı çalışmadır [123]. Bu tür özel veri kaydetme ortamından dijital delillerin adli bilişim incelemesine tabi tutulması teorik düzeyde pekala mümkündür. Aynı doğrultuda, quartz gibi özel bazı maddelere kaydedilen veriler [124]. ve bir atoma veri yazılması gibi teknolojik gelişmeler [125] adli bilişimin gelecekte ne kadar kompleks hale geleceği hususunda önemli ipuçları vermektedir.

6.4.3. Türk Hukukunda Adli Bilişim

6.4.3.1. Ceza Muhakemesi Kanununu 134. Maddesi

Türk hukukunda adli bilişimle ilgili temel düzenleme 5271 sayılı Ceza Muhakemesi Kanunu'nun "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlıklı 134. maddesi altında düzenlenmiştir. Söz konusu hükme göre bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkanının bulunmaması halinde [126], hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir. Nihayetinde, adli bilişim incelemesiyle bir kişiye ait bilişim sisteminde arama yapılmakta, kopya alınmakta ve haliyle o kişinin özel alanına müdahale edilmektedir. Bu sebepledir ki, asıl olan hâkimin, istisna ise Cumhuriyet savcısının adli bilişim incelemesi için karar vermesidir. Eğer ki, gecikmesinde sakınca bulunan bir hal durumunda Cumhuriyet savcısı karar vermişse, bu kararın yirmi dört saat içinde hâkim onayına sunulması zorunludur. Ceza Muhakemesi Kanunu'na göre hâkimin kararını en geç yirmi dört saat içinde vermesi gereklidir. Söz konusu müdahalenin temel hak ve hürriyetler üzerindeki etkisi göz önüne alınarak açık bir kısıtlama hükmü koyulmuş ve sürenin dolması veya hâkim tarafından ak-

sine karar verilmesi halinde çıkarılan kopyaların ve çözümü yapılan metinlerin derhal imha edileceği hüküm altına alınmıştır.

Ceza Muhakemesi Kanunu'nun genel yaklaşımı, adli bilişim incelemesinin olay yerinde yapılmasıdır. 134. maddenin ikinci fıkrasına göre bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilecektir. Yine aynı hükme göre şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilecektir.

134. maddenin üçüncü fıkrasına uyarınca bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesinin yapılması gereklidir. Bu hükme göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmesi ve bu husus tutanağa geçirilerek imza altına alınması da zorunludur.

Olay yerinde veya cihazın bulunduğu yerde elkoymaksızın inceleme yapılması mümkün müdür? 134. maddenin beşinci fıkrasına göre bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu hususun tutanağa kaydedilmesi ve ilgililer tarafından imza altına alınması zorunludur.

6.4.3.2. Adli Tıp Kurumu Adli Bilişim İhtisas Dairesi

Uygulamada adli bilişim incelemeleri için bilirkişilik yapacak özel yetkili bir merciinin olmaması da önemli bir sorundu. Adli bilişimin kurumsallaşması adına Türkiye'deki önemli gelişmelerden birisi 2016 yılında Adli Tıp Kurumu bünyesinde Adli Bilişim İhtisas Dairesi'nin kurulmasıdır. Söz konusu dairenin görevleri 2659 sayılı Adli Tıp Kurumu Kanunu'na eklenen 22/A maddesinde *"Mahkemeler ile hakimlikler ve savcılıklar tarafından talep edilen bilişim ile ilgili konularda gerekli incelemeleri yapmak; veri toplama, işleme, depolama veya aktarma işlevi gören bilişim sistemleri ile her türlü sayısal ve elektronik materyal üzerinde inceleme, araştırma ve analizleri yapmak, sonuçlarını bir raporla tespit etmek."* şeklinde belirtilmiştir [127].

Adli Bilişim İhtisas Dairesi, mahkemeler ile hâkimlikler ve savcılıklar tarafından talep edilen bilişim ile ilgili konularda gerekli incelemeleri yapma; veri toplama, işleme, depolama veya aktarma işlevi gören bilişim sistemleri ile her türlü sayısal ve elektronik materyal üzerinde inceleme, araştırma ve analizleri yapma, sonuçlarını bir raporla tespit etme hususunda görevlendirilmiştir. Bu daire, Veri İnceleme Şubesi, Mobil Cihazlar İnceleme Şubesi, Kriptoloji ve Elektronik Cihazlar İnceleme Şubesi, Ses ve Görüntü İnceleme Şubesi, AR-GE Şubesi, İş Tasnifi ve Önceliği Bürosu birim ve şubelerden oluşmaktadır [128].

Adli Tıp Kurumu bünyesinde Adli Bilişim İhtisas Dairesi'nin kurulması önemli bir gelişme olmakla birlikte, adli bilişimin kurumsallaşması adına adli bilişim uzmanlığının tanımlanmasına; bu konuda standardizasyona gidilerek hem kamuda hem de özel sektörde hizmet verecek güvenilir ve de bilimsel yetkinliği haiz bir meslek grubuna ihtiyaç vardır.

6.4.4. Reform Önerileri

Ceza Muhakemesi Kanunu'nun 134. maddesinde yer alan düzenleme zaman içerisinde farklı ihtiyaçları karşılamak amacıyla gerçekleştirilen değişikliklerle bugünkü halini almıştır. Kronolojik olarak yapılan değişiklikleri sıralamak gerekirse:

- 2014 yılında 6526 sayılı Kanun'un 11. maddesiyle yapılan değişiklikle adli bilişim hükmünün uygulanması için "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" şartı getirilmiştir.
- 2014 yılındaki değişiklikle istem halinde imajın şüpheliye veya vekiline verilmesi hükmü değiştirilmiş ve imajın istem olmaksızın doğrudan şüpheliye veya vekiline verilmesini öngören değişiklik gerçekleştirilmiştir.
- 2018 yılında 7145 sayılı Kanun'un 16. maddesiyle yapılan değişiklikle Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulacağı; hâkim kararını en geç yirmi dört saat içinde vereceği; sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edileceğini öngören değişiklik gerçekleştirilmiştir.

- 2018 yılındaki değişiklikle, bilgisayar, bilgisayar programları ve bilgisayar kütüklerine el konulması için aranan şartları arasına işlemin uzun sürecek olması hali eklenmiştir.

Tüm bu değişikliklere rağmen, düzenlemenin adli bilişim alanındaki tüm ihtiyaçlara cevap verdiğini söylemek zordur. Aşağıda 134. maddenin adli bilişimin gerekliliklerine cevap vermesi için reform önerileri temel hatlarıyla belirtilmeye çalışılmıştır:

(1) Uygulamada, 134. maddede yer alan bilgisayar kavramının dar yorumlanması sebebiyle bilişim sistemlerine yönelik (özellikle IoT - akıllı cihazlar, hatta bazı durumlarda akıllı telefonlar) adli bilişim incelemesi yapılamaması gibi sorunları bertaraf etmek amacıyla söz konusu hükmün her türlü bilişim sistemini kapsayacak şekilde tekrar kaleme alınması gerekir. Ayrıca, madde başlığının "Adli bilişim incelemesi" veya "Bilişim sistemlerinde adli arama, el koyma ve izleme tedbiri" şeklinde revize edilmesi amaca uygun düşecektir.

(2) Ceza Muhakemesi Kanunu, temel olarak arama koruma tedbirinden hareket etmektedir. Bilişim sistemine el koyulması için bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması gerekir. 2018 yılında yapılan değişiklikle de işlemin uzun sürecek olması yeni el koyma sebebi olarak tanımlanmıştır. Uygulamada, el koyma ihtiyacı yalnız bu durumlarda ortaya çıkmamaktadır. Terör veya örgütlü suçlarda olay yerinin fiziksel güvenliğinin teminiyle ilgili sorunlar olabilir. Fiziksel ortamda kesintisiz şekilde enerji temini sorunu yaşanabilir. Örnekler artırılabilir. Olası hukuka aykırılık iddialarını bertaraf etmek amacıyla genel bir el koyma sebebinin tanımlanması yerinde olacaktır.

(3) Arama ve/veya elkoyma tedbirinden sonra imajın bir kopyasının şüpheliye her koşulda verilmesinin çeşitli sakıncaları bulunmaktadır. Bazı suçlar için verinin bulundurulması suç teşkil etmekte veya kopyanın şüpheliye verilmesi durumunda şüphelinin suç işlemeye devam etmesi söz konusu olabilecektir. İlk durum için çocuk pornografisi içeriği; ikinci durum için ise çalınmış kredi kartı bilgilerinin olduğu durumlar örnek gösterilebilir. Bu tür içerik suçlarında içeriğin hemen teslim edilmemesi ve kovuşturmada bu konuda özel bir karar alınmasının gerekli kılınmasını gerektirecek bir düzenleme yapılmalıdır. Öte yandan, veri kaydeden medya dışında ticari

hayatta özellikle bir kesinti veya hak kaybı yaşanmaması için kovuşturmanın tamamlanmasını beklemeden cihazın kendisinin de mümkün olan en hızlı şekilde iade edilmesinin önü açılmalıdır.

(4) Ceza Muhakemesi Kanunu'nun 134. maddesinde adli bilişimle ilgili alınacak önlemlerin muhatabı olarak sadece şüpheli sayılmıştır. Bazı durumlarda mağdur veya suçta zarar görenin veya üçüncü bir kişinin de cihazının incelenmesi gerekli olabilir. Bu bağlamda, genel bir düzenleme yapılarak bu konuya açık bir normatif dayanak kazandırılmalıdır.

(5) Ceza Muhakemesi Kanunu'nun 134. maddesi uyarınca adli bilişim incelemesi yapılmasının ön koşulu bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkanının bulunmamasıdır. Korunan hukuki değerler göz önüne alınarak bu koşulların aranmadığı bazı katalog suçların belirlenmesi yerinde olacaktır. Örneğin, Türk Ceza Kanunu'nda yer alan Bilişim sistemine girme (Madde 243), Sistemi engelleme, bozma, verileri yok etme veya değiştirme (Madde 244), Banka veya kredi kartlarının kötüye kullanılması (Madde 245), Yasak cihaz veya programlar (Madde 245/A), Kişisel verilerin kaydedilmesi (Madde 135), Verileri hukuka aykırı olarak verme veya ele geçirme (Madde 136) gibi suçlara bu bağlamda özel bir statü tanınabilir ve makul şüphenin varlığı yeterli görülüp, başka surette delil elde etme imkanının bulunmaması şartı aranmayabilir.

(6) Adli bilişim alanında tartışmalı bir diğer sorun ise imajlarla veri analitiği yapılıp yapılamayacağıdır. Özellikle örgütlü suçlarda, örgüt üyelerinin tespiti, iletişimi veya işbirliği bakımından bu konu önem arz etmektedir. Örneğin, bir soruşturma sırasında bir şehirde ele geçirilen bir bilişim sisteminde yer alan ve özgün isimli bir terör içerikli dosyanın başka bir soruşturmada da tespit edilmesi suretiyle her iki soruşturma arasında korelasyon kurulabilir ve bu dosyalar örgütsel ilişkinin tespiti bakımından yol gösterici olabilir. Bu analitik çalışmanın yapılması için dosyanın kendisinin birebir kopyalanmış olması da gerekmez. Dosyanın hash değerli boyutu ve tam dosya isimlerinin karşılaştırılması bile yeterlidir. Bu şekilde bir incelemeyle bir dosyanın izinin sürülmesi, örgütsel yapının bilgi alışverişi hususunda önemli bilgilere ulaşılması pekâlâ mümkündür. Ancak, bu tür incelemenin yapılabilmesi için dosya isimleri ve

boyutlarının hashli halinin ortak bir havuzda toplanması, işlenmesi ve ilgili adli bilişim birimlerine aktarılması gerekmektedir. Dosya analitiğinin faydaları yadsınamıyorsa da konunun kişisel verilerin ve mahremiyetin korunması, tedbirlerin geçiciliği, kopyalar ve çözümü yapılan metinlerin imha edilmesini gerektiren durumlar ve ölçülülük perspektiflerinden ayrı ayrı ele alınması ve bu doğrultuda, temel hak ve hürriyetler üzerindeki etkisi sebebiyle açık şekilde kanunla düzenlenmesi gerekmektedir.

6.5. Değerlendirmeler

Dünyada siber güvenlik tehditleri artmakta, şekil ve nitelik değiştirmekte, etkilediği alanlar farklılaşmaktadır. Siber tehditlerle mücadele dinamik bir metodoloji gerektirmektedir. Klasik yöntemlerle bu tehditlere karşı konulması mümkün değildir. Siber tehditlerin coğrafi sınır tanımaması, çok az masrafla, çok kısa sürede büyük zararlara yol açabilecek şekilde işlenmesi ve faillerin çoğu zaman bu suçlarda anonim olması nedeniyle bilişim suçlarının soruşturmasında ve kovuşturmasında kullanılan yöntem ve tekniklerin gözden geçirilmesi gerekmektedir.

Bilişim suçlarının kapsamlı incelemeye alındığı ikinci bölümde incelendiği üzere, Türk Ceza Kanunu, Bilişim sistemine girme, Sistemi engelleme, bozma, verileri yok etme veya değiştirme, Banka veya kredi kartlarının kötüye kullanılması, Yasak cihaz veya programlar maddeleri altında müstakil bilişim suçlarını düzenlemekte ve farklı suçlar altında da bilişim sisteminin bir aracı olarak kullanılmasını (nitelikli hırsızlık ve nitelikli dolandırıcılık gibi) nitelikli hal olarak cezalandırmaktadır.

Bilişim suçları farklı hükümler altında düzenleniyor olsa da, söz konusu suçlar iç içedir. Öyle ki, bir bilişim sistemine girme durumunda veriler taksirle yok olur veya değişirse bilişim sistemine girme suçu söz konusu olabilirken, veriler kasten yok edilir veya değiştirilirse müstakil bir suç olan Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu söz konusu olabilmektedir. Aynı doğrultuda, bilişim sistemleri arasında ayrım yapılmakta, bazen bu ayrım neticesinde ceza indirimine gidilmekte (bedeli karşılığı yararlanılabilen sistemler gibi) bazen ise bilişim sisteminin kamusal önemi sebebiyle (bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemleri gibi) ceza artırılmaktadır. Tüm bunların

ötesinde, ilgili yerlerde açıklandığı üzere, bilişim sisteminin tanımı ve kapsamı da tartışmalıdır ve farklı yorumlarla çelişkili uygulamalar söz konusu olabilmektedir.

Bilişim suçlarının muhakemesinin diğer suçlara nazaran daha hızlı şekilde tamamlanmasında bilişim sistemlerinin modern hayatın en temel bileşeni haline gelmesi sebebiyle üstün bir kamusal yarar vardır. Ayrıca, kanun koyucunun bu alanı yakından gözlemleyerek, yeni gelişmelere hızlı şekilde reaksiyon göstermesi ve güncel risk ve tehditleri bilişim suçlarının tanımına koyması gerekmektedir. Tüm bu süreçte bütüncül bir yaklaşımın sergilenmesi ve yapılan düzenlemelerin, Türkiye'de gelişim aşamasında olan siber güvenlik alanını ölçüsüz şekilde kısıtlamaması gerekir.

Tüm incelemeler ışığında, bilişim suçlarının Türk Ceza Kanunu'nun "Topluma Karşı Suçlar" başlıklı Üçüncü Kısım'ında "Bilişim Alanında Suçlar" başlıklı Onuncu Bölümünde yer alan müstakil suçların sadeleştirilmesi gerekmektedir. Rasyonelleştirilmiş sadeleştirilme kapsamında, birbiriyle bağlantılı Bilişim sistemine girme ile sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarının tek bir başlık altına toplanması; suçun manevi unsurlarına açıklık getirilmesi, hukuka uygunluk sebeplerinin uygulama dikkate alınarak hukuki belirlilik açısından daha açık tanımlanması; bilişim sistemlerinin tanımına açıklık getirilmesi ve bu tanımın mümkün olduğunca geniş tutulması yerinde olacaktır. Bu sadeleştirme karşısında, suçlar için öngörülen cezalarının marjının artırılması ve mümkün olduğunca adli para cezası temelli bir sistemin getirilmesi önerilmektedir.

Önerilen sistemde, hükmü uygulayacak olan hâkime geniş bir takdir yetkisi verilmektedir. Suçun işleniş amacı, bilişim sistemine yönelik eylemler neticesinde ortaya çıkan zararın bireysel ve toplumsal etkisi, zararın telafisinin mümkün olup olmadığı gibi unsurlar dikkate alınarak bireysel zarar durumunda adli para cezası, toplumsal zarar durumunda hapis cezası temelli bir yaklaşım geliştirilmelidir.

Nitekim, Türk Ceza Kanunu'nun 61. maddesi uyarınca hâkim, failin güttüğü amaç ve saiki göz önünde bulundurarak, işlenen suçun kanuni tanımında öngörülen cezanın alt ve üst sınırı arasında temel cezayı belirler. Aynı doğrultuda, Türk Ceza Kanunu'nun 62. maddesi takdiri indirim nedenlerine yer verirken, takdiri indirim nedeni

olarak, failin geçmişi, sosyal ilişkileri, fiilden sonraki ve yargılama sürecindeki davranışları, cezanın failin geleceği üzerindeki olası etkileri gibi hususlar göz önünde bulundurarak takdir yetkisini haizdir. Bilişim suçları bakımından önemli olan husus olarak, bilişim sistemindeki açığın, zafiyetin veya riskin fail tarafından mağdurla paylaşılması, söz konusu fiilin nasıl gerçekleştirdiği konusunda teknik olarak yol göstermesi, bu şekilde bilişim sisteminin gelecekteki saldırılara ve risklere karşı korunmasına yardımcı olması şeklindeki samimi hareketlerinin cezanın takdiri indirim nedenlerinin uygulanmasında özellikle değerlendirilmesi kritik önemi haizdir. Bu şekilde, toplumsal faydanın en üstün şekilde sağlanması mümkün olacaktır.

Son olarak, bilişim suçlarının soruşturulması ve kovuşturulması için müstakil bilişim ihtisas mahkemelerinin kurulması gerekmektedir. 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı da bilişim suçlarıyla mücadelenin etkinleştirilmesi amacıyla bilişim ihtisas mahkemelerinin kurulmasını, bu mahkemelerde görev yapan yargı personelinin yetkinliğinin arttırılması için gerekli tedbirlerin alınmasını hedefleri arasında saymıştır [129]. Bilişim ihtisas mahkemelerinden beklenen faydanın sağlanabilmesi için, tüm sürecin klasik usulle yürütüldüğü, klasik bir görev ayrımına dayalı bir mahkemeden ziyade; işin ruhuna uygun düşen dijital yargılamaya geçilmesi gerekir. Öyle ki, şikayetin doğrudan çevrimiçi yapılmasının mümkün olması, delillerin toplanmasında dijital keşif uygulamalarından faydalanılması, duruşmaların dijital ortamda yapılması ve tüm süreçte bilişim teknolojilerinin tüm olanaklarından faydalanılması gerekir. Bu konuda dünyada başarılı uygulamalar vardır. Dünya Fikri Mülkiyet Örgütü (WIPO) alan adları için uzun bir süredir online tahkim uygulamasını etkin şekilde uygulamaktadır [130]. Nitekim, Çin Halk Cumhuriyeti daha da öteye geçerek ve öncü olarak, yakın zamanda the Hangzhou Internet Court isimli çevrimiçi mahkemeyi hizmete sunmuştur [131]. Bilişim uyuşmazlıklarının Türkiye'de de bilişimin ruhuna uygun şekilde hızla neticelendirilmesi için bir an evvel hem medeni yargı hem de ceza yargısı alanlarında çevrimiçi bilişim ihtisas mahkemelerinin kurulması zaruridir.

Kaynaklar

[*] Bu çalışma kapsamında atıf yapılan tüm elektronik ağ adreslerinin güncelliği, 1 Kasım 2018 tarihinde tekrar erişilmek suretiyle teyit edilmiştir. Bu sebeple, dipnotlarda müstakil erişim tarihleri belirtilmemiştir.

[1] Stouffer, K., Falco, J., ve Ken, K. (2007) *Guide to Supervisory Control and Data Acquisition (Scada) and Industrial Control Systems Security 'Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology, Technology Administration US Department of Commerce, s. 6; Ayrıca bkz. Cyber Threat Source Descriptions URL: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#nat.

[2] Koca, M., Üzülmez, İ. (2016) *Türk Ceza Hukuku Özel Hükümler*. Ankara: Adalet Yayınevi, s. 801.

[3] Avrupa Konseyi Siber Suçlar Sözleşmesi'nin hazırlık süreçleri ve kapsamı için bkz. Önok, M. (2013) *Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği*. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 19(2), 1229-1269; Keskin, S. (2011) *Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 59(1-2) 155-180.

[4] Çekinceler ve sözleşme metni için bkz. URL: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf.

[5] Chart of signatures and ratifications of Treaty 185 URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=oiBOGx95.

[6] Bu konuda özellikle bkz. Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 206 dn. 11.

[7] Bilişim sisteminin güvenliği için bkz. Dülger, M. V. (2015) *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin, s. 348; bilişim sisteminin güvenilirliği için bkz. Özbek, V.Ö., Doğan, K., Bacaksız, P., Tepe, İ. (2016) *Türk Ceza Hukuku Özel Hükümler*. Ankara: Seçkin Yayıncılık, s. 932.

[8] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 348.

[9] *Özbek/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler*, s. 933.

[10] Bu konuda kapsamlı bir inceleme için bkz. Zengin, M.A. (2013) *Bilgi İletişim Teknolojilerinin Demokrasi İçerisinde Kullanımı ve Dijital Demokrasiye Geçiş*. Gazi Üniversitesi Hukuk Fakültesi Dergisi, 17(4), 271-304.

[11] Avrupa Birliği e-Devlet Eylem Planı 2016-2020 için bkz. Communication from the Commission to the European Parliament, the Council,

the European Economic and Social Committee and the Committee of the Regions: EU eGovernment Action Plan 2016-2020 Accelerating the digital transformation of government (COM(2016) 179 final) URL: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15268; aynı doğrultuda e-Devlet Ekosisteminin Etkinliğinin ve Sürdürülebilirliğinin Sağlanması stratejik amacının altında e-Devlet Kurumsal Mimarisinin Oluşturulması Eylem Planı için bkz. Ulusal e-Devlet Stratejisi ve Eylem Planı (2016-2019), Resmi Gazete 19.07.2016/29775 (Mükerrer).

[12] E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik, Resmi Gazete 03.09.2016/29820.

[13] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 809.

[14] Özbek/Doğan/Bacaksız/Tepe, *Türk Ceza Hukuku Özel Hükümler*, s. 934.

[15] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 809.

[16] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 360.

[17] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 360.

[18] Koca, M., Üzülmez, İ. (2016) *Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayıncılık, s. 112.

[19] Artuk, M. E., Gökcen, A., Yenidünya, C. (2016) *Ceza Hukuku Genel Hükümler*. Ankara: Adalet Yayınevi, s. 285.

[20] Yeni TCK Madde Gerekçeleri, URL: http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc.

[21] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 810.

[22] Artuk, M. E., Gökcen, A., Yenidünya, C. (2015) *Ceza Hukuku Özel Hükümler*. Ankara: Adalet Yayınevi, s. 870; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 73-77.

[23] Bu konuda kapsamlı ve güncel bir inceleme için ayrıca bkz. Açıkgöz, E. İ. (2018) *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlam Suçu, Yüksek Lisans Tezi, Ankara Yıldırım Beyazıt Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Yüksek Lisans Programı, Ankara.*

[24] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 812.

[25] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 812.

[26] Demirbaş, T. (2016) *Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayıncılık, s. 245.

[27] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 362.

[28] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 813.

[29] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 363.

[30] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 813; bu konudaki tartışmalar ve düzenlemelerin yerindeliği için özellikle bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 360.

[31] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 813.

[32] Bu konudaki tartışmalar için bkz. Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 811 ve özellikle dn. 32.

[33] Artuk/Gökcen/Yenidünya, *Ceza Hukuku Özel Hükümler*, s. 862; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 362.

[34] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 365-366.

[35] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 365.

[36] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 814.

[37] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 816.

[38] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 376.

[39] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 375.

[40] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 118.

[41] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 374.

[42] Karagülmez, A. (2014) *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri*. Ankara: Seçkin Yayıncılık, s. 212.

[43] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 817.

[44] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 817; Karagülmez, *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri*, s. 212; Öte yandan, failin bilişim sistemine girmesi ve sistemde kalmaya devam etmesi eyleminin neticesi olarak sistemdeki verilerin yok olması veya değişmesi halinde, fail ister taksirle, ister kasıtla bu neticeye sebebiyet versin 243. maddenin 3. fıkrasını ihlal etmiş olacağı; failin sistemdeki verilerin yok olmasına ya da değişmesine yol açan hareketini kasıtla yapması halinde aynı zamanda 244. maddenin 2. fıkrasında tanımlanan suç da gerçekleşmiş olacağı; bu durumda failin tek eylemiyle yasanın birden fazla normunun ihlal edilmiş olması gündeme geleceği için düşünsel birleşme (fikri içtima) söz konusu olacağı ve Türk Ceza Kanununun 44. maddesi gereğince cezası daha ağır olan norm somut olaya uygulanacağı, 244/2'nin cezası daha fazla olduğu için bu maddenin uygulanması gerekeceği ileri sürülmektedir. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 372.

[45] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 817.

[46] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 372.

[47] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 372.

[48] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 814.

[49] Artuk/Gökcen/Yenidünya, *Ceza Hukuku Özel Hükümler*, s. 876.

[50] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 262-263.

[51] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 392; Gazetecilik mesleiğinin icrasının sisteme izinsiz girmek için hakkın kullanılması hukuka uygunluk nedeni oluşturup oluşturmayacağı için kapsamlı bir inceleme için bkz. Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 392-394.

[52] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 392.

[53] DDOS hakkında kapsamlı bilgi için bkz. Ryan, J. (2010) *A History of the Internet and the Digital Future*. London: Reaktion Books, s. 194.

[54] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 327.

[55] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 391.

[56] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 324.

[57] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 327.

[58] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 328.

[59] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 391.

[60] Rızada ehliyet konusu için bkz. Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 325.

[61] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 391.

[62] Gri-şapkalı hackerlarle ilgili güncel bir çalışma için bkz. Harper, A., Harris, S. Ness, J., Eagle, C., Lenkey, G., Williams, T. (2011) *Gray Hat Hacking - the Ethical Hacker's Handbook*. New York: McGraw-Hill.

[63] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 309.

[64] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 262-263.

[65] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 268.

[66] Centel, N., Zafer, H., Çakmut, Özlem (2016) *Türk Ceza Hukukuna Giriş*. İstanbul: Beta Yayıncılık, s. 291-293.

[67] Demirbaş, *Ceza Hukuku Genel Hükümler*, s. 450.

[68] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 817.

[69] Zincirleme suçun hukuki niteliği hakkında ileri sürülen diğer bir görüş ise suç çokluğu görüşüdür. Buna göre, zincirleme suç gerçekte her biri bağımsız nitelikte olan birden çok suçtan meydana gelmiştir. Sırf pratik gereklerle, yani cezaların toplanmasının şiddetini azaltmak için bu müessese kanunda düzenlenmiştir. Bu konuda bkz. Koca/Üzülmez, *Türk Ceza Hukuku Genel Hükümler,* s. 499.

[70] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 402.

[71] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 402.

[72] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 818.

[73] Artuk/Gökcen/Yenidünya, *Ceza Hukuku Özel Hükümler*, s. 878.

[74] Artuk/Gökcen/Yenidünya, *Ceza Hukuku Özel Hükümler*, s. 878.

[75] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 819.

[76] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 821.

[77] Akbulut, B. (2017) *Bilişim Alanında Suçlar*. Ankara: Adalet Yayınevi, s. 165.

[78] Akbulut, *Bilişim Alanında Suçlar,* s. 163.

[79] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 822.

[80] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 822.

[81] Akbulut, *Bilişim Alanında Suçlar*, s. 168.

[82] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 822.

[83] Akbulut, *Bilişim Alanında Suçlar*, s. 168.

[84] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 823.

[85] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 823.

[86] Akbulut, *Bilişim Alanında Suçlar*, s. 170.

[87] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 825.

[88] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 823.

[89] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* s. 417-418.

[90] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 829; Özbek/Doğan/Bacaksız/Tepe, *Türk Ceza Hukuku Özel Hükümler*, s. 923; Ketizmen, M. (2008) *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Adalet Yayınevi, s. 139.

[91] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları,* s. 140.

[92] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* s. 830.

[93] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 830.

[94] Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 428.

[95] Özbek/Doğan/Bacaksız/Tepe, *Türk Ceza Hukuku Özel Hükümler*, s. 954.

[96] Artuk, M. E., Gökcen, A. (2017) *Ceza Hukuku Özel Hükümler*. Ankara: Adalet, s. 891; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 439; Gürler, F. (2015) *Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar*. Ankara: Yetkin Yayınları, s. 148; Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 834.

[97] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 833.

[98] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 872.

[99] Akbulut, *Bilişim Alanında Suçlar*, s. 353-354.

[100] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 873.

[101] Akbulut, *Bilişim Alanında Suçlar*, s. 358-359.

[102] Koca/Üzülmez, *Türk Ceza Hukuku Özel Hükümler*, s. 875.

[103] Resmi Gazete 20.10.2012/28447.

[104] 15.08.2016 tarihli ve 671 sayılı Kanun Hükmünde Kararnameyle 5651 sayılı Kanuna eklenen Ek Madde 3 ile Telekomünikasyon İletişim Başkanlığı kapatılmış; bu idari birimin tüm görev ve yetkileri Bilgi Teknolojileri ve İletişim Kurumu'na devredilmiştir.

[105] Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, Resmi Gazete 11.11.2013/28818.

[106] 2016-2019 Ulusal Siber Güvenlik Stratejisi, URL: http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf.

[107] ISO/IEC 27037:2012 - Information technology — Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence, URL: https://www.iso.org/standard/44381.html; ayrıca bkz. ISO/IEC 27037:2012 - Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence, URL: http://www.iso27001security.com/html/27037.html.

[108] ISO/IEC 27037:2012 - Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence, URL: https://www.iso.org/standard/44381.html.

[109] ISO/IEC 27041:2015, Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method, URL: https://www.iso.org/standard/44405.html.

[110] ISO/IEC 27042:2015, Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence, URL: https://www.iso.org/standard/44406.html.

[111] ISO/IEC 27043:2015 Information technology - Security techniques - Incident investigation principles and processes, URL: https://www.iso.org/standard/44407.html.

[112] ISO/IEC 27050-1:2016 Information technology - Security techniques - Electronic discovery - Part 1: Overview and concepts, URL: https://www.iso.org/standard/63081.htm.

[113] Adli bilişimin safhaları için bkz. Keser Berber, L. (2004) *Adli Bilişim (Computer Forensic)*. Ankara: Yetkin Yayınları, s. 67-74.

[114] Keser Berber, *Adli Bilişim (Computer Forensic),* s. 44.

[115] Keser Berber, *Adli Bilişim (Computer Forensic),* s. 44.

[116] Keser Berber, *Adli Bilişim (Computer Forensic),* s. 41.

[117] Keser Berber, *Adli Bilişim (Computer Forensic),* s. 100.

[118] Fitbit verisinin bir kadının tecavüz iddiasını çürütmek için kişi aleyhine delil olduğu bir örnek için bkz. Fitbit data just undermined a woman's rape claim URL: https://splinternews.com/fitbit-data-just-undermined-a-womans-rape-claim-1793848735.

[119] Bu konuda kapsamlı bir inceleme için bkz. Hegarty, R. C., Lamb, D., Attwood, A. (2014) *Digital Evidence Challenges in the Internet of Things*. Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis, Salzburg, Austria.

[120] Bu konuda güncel bir çalışma için bkz. Tully, M. (2016) *The Forensic Challenges Presented by Raspberry Pi Investigation*, URL: https://computing.derby.ac.uk/c/wp-content/uploads/2016/05/The-forensic-challenges-presented-by-Raspberry-Pi-investigation.pdf.

[121] Bulut bilişimde adli bilişim incelemelerinde güncel sorunlar için bkz. Pichan, A., Lazarescu, M., Soh, S.T. (2015) *Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis*. Digital Investigation 13(1), 38-57.

[122] Amerika Birleşik Devletleri'nin 2018 yılında yürürlüğe koyduğu bulut bilişimle ilgili düzenleme bu konuda önem arz etmektedir. Bkz. the Clarifying Lawful Use of Overseas Data Act (CLOUD Act, S. 2383, H.R. 4943) URL: https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf.

[123] Goldman, N., Bertone, P., Chen, S., Dessimoz, C., LeProust, E. M., Sipos, B., Birney, E. (2013) *Toward Practical High-Capacity Low-*

Maintenance Storage of Digital Information in Synthesised DNA. Nature 494(7435), 77-80.

[124] Data Saved in Quartz Glass Might Last 300 Million Years, URL: https://www.scientificamerican.com/article/data-saved-quartz-glass-might-last-300-million-years/.

[125] IBM Turned A Single Atom Into A Tiny Hard Drive, URL: https://techviral.net/ibm-turned-single-atom-tiny-hard-drive/.

[126] Başka surette delil elde edilmesi imkanının bulunmaması hali Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin 'Tanımlar' başlıklı 4. maddesinin birinci fıkrasının (c) bendinde "*Başka suretle delil elde edilmesi imkanının bulunmaması hâli: Soruşturma veya kovuşturma sırasında diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı hususunda bir beklentinin varlığı veya başka yöntemlerden biri veya birkaçının uygulanmasına rağmen delil elde edilememesi ve delillere ancak bu Yönetmelikte düzenlenen tedbirlerle ulaşılabilecek olması"* şeklinde tanımlanmıştır. Benzer bir koruma tedbirine ilişkin bu tanım, yol gösterici olacaktır, Resmi Gazete 14.02.2007/26434.

[127] Olağanüstü Hal Kapsamında Bazı Düzenlemeler Yapılması Hakkında Kanun Hükmünde Kararname, Karar Sayısı: KHK/674 ile 2659 sayılı Adli Tıp Kurumu Kanununa eklenen 22/A maddesi, Resmi Gazete 01.09.2016/29818 (2. Mükerrer).

[128] Adli Tıp Kurumu, İdari Yapı - İhtisas Daireleri, URL: http://www.atk.gov.tr/adli-tip-ihtisas-daireleri.html.

[129] 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı, Resmi Gazete 06.03.2015/29287 (Mükerrer), URL: http://www.resmigazete.gov.tr/eskiler/2015/03/20150306M1-2-1.pdf.

[130] World Intellectual Property Organization - On-Line Arbitration URL: http://www.wipo.int/amc/en/arbitration/online/index.html.

[131] The litigation platform of Hangzhou Internet Court URL: https://www.netcourt.gov.cn/portal/main/en/index.htm.

Bilişim Suçlarında Adli Tıp Bilirkişiliği

BÖLÜM 7

Prof. Dr. Yaşar BİLGE

BİLİŞİM SUÇLARINDA ADLİ TIP BİLİRKİŞİLİĞİ

Günümüz insanının yaygın olarak kullandığı, hatta vazgeçemediği alan bilişimdir. Temel insan haklarının korunma alanlarından biri de bilişim alanıdır. Konunun farklı yönlerini vurgulayarak bu alanda süreç geliştirme amaçlanmıştır. Bu alanda yapılan ihlalleri bilirkişi kanunlar gereği delil sunarak mahkemeye görüş açıklamaktadır. Verilerin çoklu olması farklı yer ve zamanda sunulması veri analizi ile ilgili süreç de geliştirmemizde fayda bulunmaktadır. Kişisel verilerin korunması gerekir. Takdiri delil olarak sunulan bilirkişilikle ilgili belgelerin standardize edilmesi gerekir. Bilişim alanında karşılaşılan suçlar verilerle ilgili eser haklarına aykırılık, siber saldırı, hakkın kötüye kullanılması, sahtekarlık, dolandırıcılık, insan onuruna aykırı içerik ile ilgili insan ticareti, cinselliği, ekonomik saldırı ve haksız kazanç, terörle ilgili organize fiillerdir. Bilişim aracılığı ile internet bağımlılığı, kumar oynadığı, nefret suçları da toplumu etkilemektedir. Bu alandaki etkinlikler kaydedilir. Kayıt dışı durumlarda yetkililer bilgilendirilir. Yetkili kurumlar eş değerli akredite sistemle etkinlikte bulunur. İnternet ortamına suçla ilgili konunun sunulmasından vazgeçirme esastır. Hukuki açıdan sunulan durumların ortadan kaldırılması, engellenmesi, suçluların cezalandırılması gerektiği kanaatine varılmıştır.

7.1. Giriş

Konu tanım ve amaç, bilirkişilikte hukuki yön, bilirkişilikte karşılaşılan sorunlar ve çözümleri, bilişim suçlarında inceleme yöntemleri, tarihçe, veri madenciliği, sıklık ve önem, siber suçlar ve suç tipleri, ülkemizde internet üzerinden en çok işlenen suç tipleri, kişinin bilişim aracılığı ile bağımlı olduğu, kumar oynadığı, nefret suçu

işlediği, saplantılı durumu, internet bağımlılığı, önleme ve sonuç başlıkları altında incelenmiştir.

Avrupa İnsan Hakları Sistemine göre haklarımız siyasi hesap verebilirlik, azınlıkta kalan görüş ve grupları koruma, reform tetikleme, birey odaklı korumadır [1]. Mahremiyet bireyin yalnızlık, mahrem ilişki, anonimlik ve kendini sakınması alanlarındadır [2]. Bu tanımlanan hakların bilişim alanında ihmali, istismarı, kişiye zarar verilmesi hallerinde bilişim suçları söz konusudur. Hukuki zararın tanımlanmasında bilirkişinin görev ve sorumluluklarının belirtilmesi amacı ile bu derleme hazırlanmıştır.

Adli bilişim bilgisayar adli bilişimi, ağ ve internet, gömülü cihazlara ait adli bilişim olmak üzere üç grupta incelenebilir. İnceleme yöntemleri bilgisayar, ağ, mobil, GPS, medya araçları, sosyal ağ ve uzaktan arama olarak tanımlanmıştır [3]. Delilin gerçekçi, kabul edilebilir, gerçek ve aslına uygun, eksiksiz, tam, güvenilir, inanılabilir, temsil edici, akılcı, elde edilebilir, kanuna uygun elde edilmiş ve müşterek özellikleri olması gerekir [4].

7.2. Bilirkişilikte Hukuki Yön

Bilirkişi bir sorunun çözümü için uzmanlığı, özel veya teknik bilgiyi gerektiren hallerde oy ve görüşünü sözlü ya da yazılı olarak vermesi için başvurulan gerçek veya tüzel kişi olarak tanımlanabilir.

Bilirkişi olma koşullarına göre alanında en az 5 yıl çalışmış, bilirkişi eğitim belgesi bulunur. Bilirkişilikle ilgili diğer koşullar http://bilirkisilik.adalet.gov.tr/sayfalar/bilirkisili%C4%9Fekabulevebilirkisilikbasvuru.html adresinde belirtilmiştir.

7.2.1. Bilirkişi Görevleri

1) Bilirkişi yemin etmeli. Değerlendirme yaparak oy vermeli. Eğer oy birliği yoksa muhalefet şerhi koymalıdır.
2) Rapor bilirkişinin tespit ettiği objektif bulgulara, konsültasyonlar ve tetkik sonuçlarının incelenmesi ile meslekî bilgileri ışığında yapılacak değerlendirmelere dayalı ve tarafsız olmalıdır.
3) Raporlar, kesinlikle resmi makamların istek yazısının altına yazılmamalı, ayrı bir belge olarak düzenlenmelidir.
4) Raporlar el yazısı, daktilo veya bilgisayar çıktısı şeklinde verilebilir. Okunaklı olmalıdır. Özellikle sonuç kısmında anlaşılır ve

sade bir dil kullanılmalıdır. Kelimeler kısaltma yapılmadan tam olarak yazılmalıdır. Kısaltma yapılacaksa ilkine parantez içinde anlam açıklamalı yapılmalıdır.

5) Raporun ilk sayfasında değerlendirmeyi yapan kuruluşunun ismi; raporun her sayfasında muayene edilen kişinin adı, soyadı ve raporu düzenleyen tabibin parafı veya imzası; raporun sonunda okunaklı olarak raporu düzenleyenin adı, soyadı, diploma numarası ve imzası bulunmalıdır.
6) Adlî kanıt niteliği taşıyan tetkik sonuçları ve grafilerin aslı, muayene edilen kişinin kendisine verilmemeli ve ilgili mevzuatta belirtilen süreyle arşivde saklanmalıdır. Bu materyallerin, özellikle grafilerin üzerinde muayene edilenin adı, soyadı ve kayıt numarası silinmeyecek ve değiştirilmeyecek şekilde yer almalıdır. Kopya belgelerin aslı gibi olduğu kaydedilmelidir. Belgeler tutanakla yetkili kişiye teslim edilmelidir.
7) Danışman, konsültasyon raporları öğretim üyesi düzeyinde yapılmalıdır.
8) Kesin rapor tanzimine uygun olmayan durumlarda kesin rapor tanzimi için gerekli incelemelerin gerekli ise ne zaman, hangi kurum tarafından hangi incelemelere göre tanzim olunacağına dair bilgiler geçici raporda kaydedilmelidir.
9) Düzenlenen raporlar adlî rapor kayıt defterine, raporun sonuç kısmındaki değerlendirmeler yer alacak şekilde kaydedilmelidir.
10) Bilirkişi raporları üç nüsha olarak; biri kuryeye, biri arşive diğeri de gitmeme veya raporun teslim edilmeme olasılığı varsa posta havalesi ile ilgili merciye gönderilecek tarzda düzenlenmelidir.
11) Ceza Muhakeme Kanununun 86ncı maddesine göre ölü kimliğini belirlemek ve adlî muayene yapmak, 87nci maddesine göre otopsi yapmak, 88inci maddesine göre yeni doğanın cesedinin adlî muayenesini veya otopsisini yapmak ve 89uncu maddesine göre de zehirlenme şüphesi üzerine inceleme yapmak gerekir.

7.2.2. Kabul Edilebilirlik

Başvurunun incelenebilir özellikleri şunlardır:

1) Erişilebilirlik

2) Hasta-hizmet sunucu ilişkisi: Beklenen faydaya uygundur.
3) Hizmet konfor sağlayan yönü
4) Risk ve maliyet
5) Adalet ve hakkaniyet

7.2.3. Bilirkişi Raporuna Yapılan İtiraz Sebepleri

1) Bilirkişi rapor düzenlediği konuda uzman olmaması, uzmanlık alanının farklı olması
2) Bilirkişinin reddini gerektiren durum varsa
3) Bilirkişi raporunun gerçeği yansıtmaması
4) Bilirkişiye sorulan soruların net olarak açıklanmaması
5) Raporda verilmesi gereken bazı sorulara cevap verilmemesi
6) Bilirkişinin raporda hesaplama ve işlemde hatası yapması
7) Bilirkişinin Adli Yargı Adalet Komisyonu Listesinden seçilmiş olması hali
8) Bilirkişinin taraflı olması

7.2.4. Bilirkişilikle İlgili Sorunların Çözümleri

7.2.4.1. Bilirkişiyi Sorumlu Kılma

Bilirkişinin görevi, davet üzerine gittiğinde görüşünü sözlü veya yazılı olarak bildirmemesi, verilen zamanda yanıt vermemesi (iki aydan az sürede) davetiyeye rağmen görüş açıklamaması halinde (CMK. m 46, 63, 70) ve HUMK m 271 ve 278`inci maddelerine göre yargılanır. Görevini kötüye kullanmada TCK m 257, göreve ilişkin sırrı açıklamada TCK m 258; kamu görevini yapmama halinde TCK m 260, gerçeğe aykırı bilirkişilikte TCK m 276, kamu görevlisinin suçu bildirmemesi halinde TCK m 279-280; suç delillerini yok etme-gizleme-değiştirmede TCK m 281, suçluyu kayırma halinde TCK m 283, soruşturmanın gizliliğini ihlalde TCK m 285, ses ve görüntüyü kayda alan yetkisiz kişiye TCK m 286, genital muayene yetkili hakim veya savcı kararı olmaksızın yapılırsa TCK m 287, adil yargılamayı etkilemeye teşebbüs etme halinde TCK m 288 hükümleri uygulanır.

7.2.4.2. Sorulan Soru

Doğru, etkin olmalı. Soru ihtiyaç ve beklentiyi gidermeye uygun nitelikte olmalıdır. Sorunun amacı genel bir sorunu çözmeye yönelik olmalı. Soru özel bir durumu, ayrıntılamaya yöneliktir. Sonuç vericidir. Güncel veya kanuna uygun bir durumu tanımlatmaya yöneliktir. Somut olayı anlamaya elverişlidir. Sorular kendi içerisinde tutarlı olmalıdır. Sorular mantıki açıdan somuttan soyuta; basitten karmaşığa; bilinenden bilinmeyene doğrudur.

7.2.4.3. Dosya Düzenlemesi

Genellikle tarihi sıralamalıdır. Bunun yanı sıra grup halinde ifade tutanakları; iddianame, mahkeme celseleri; bilirkişi raporları tarzında da alt başlıklar halinde sıralama yapılabilir.

Raporla ilgili: Rapor geçerliliği olan inandırıcı, oluşa uygun ve vakalara dayalı olmalıdır. Buna göre:

Tanımlama kriterlerinin özgün ve nesnel olması gerekir.

Uygulanan metot ve materyal: Sorulan soruya, sorunun içeriğine, ortama uygun metot kullanılması gerekir. Metodun uygulanmasına yarayan araçlarla ilgili sorunlar şöyle giderilebilir:

Araç standarta ve amaca uygun niteliktedir. Teknik şartnamesi, proforması alınmıştır.

7.2.4.4. Delil

1. Hakim delili takdir ederek (CMK m 217) kabul eder.
2. Delil yasalara uygun olarak elde edilmelidir.
3. Suçu ispatlamaya elverişli olmalıdır. Suçla ilgili yeterli kanaat uyandırmalıdır.
4. Delil gerçekçi ve akılcı olmalıdır.
5. Maddi vakayı yansıtmalıdır.
6. Yapay müdahale olmadıkça tanınmayacak şekilde değiştirilme imkanı olmamalıdır.
7. Benzerlerinden ayırt edici özelliği olmalıdır.
8. Arşivde belli sistemle saklanabilir olmalıdır.

9. Nedensellik bağını g*östermelidir. Sanığın suçu kabulde veya itiraf etmesinde etkili olmalıdır. Suçun işleniş zamanı, yöntemi, nedeni, nasıl olduğu hakkında bilgi verici olmalıdır. Delil olaya nesnel ve öznel olmalıdır.*

Delil'in Reddi Gerekenler Durumlar Şunlardır (CMK M 206):

1. *Delil kanuna aykırı elde edilmişse;*
2. *Delil ile ispat edilmek istenen olayın karara etkisi yoksa;*
3. *İstem sadece davayı uzatmak maksadıyla yapılmışsa [5]*

7.3. Bilişim Suçlarında İnceleme Yöntemleri

Yazılımları incelemede Encase Forensics, Forensic Tool Kit, ProDiscover, SMART, The Sleuth Kit/autopsy; donanımları ise Tableau yazma-koruma cihazları, Voom Teknoloji cihazları Solo-III kopyalama cihazları kullanılabilir [6]. Adli kopyanın orijinal delil üzerinden alınması ve kopya üzerindeki değişiklik hash hesaplatılması ile yapılması gerekir [6,7,8]. CMK 134. Maddesinin hash değeri, şüpheli hakları, ceza soruşturmasının selameti açısından yeniden düzenlenme gereği açıklanmıştır [3].

7.4. Tarihçe

Amerika'da 1986 yılında Elektronik Haberleşme Gizlilik Kanunu çıkartılmıştır. 1988 yılında Fransız Ceza Kanununda bilişim suçlarına ait düzenleme yapılmıştır. 1997 yılından itibaren kanuni düzenlemeler avrupa ve dünyada geliştirilmiştir. Ülkemizde 1999 yılında Bilişim Suçları Şube Müdürlüğü kurulmuş, 2002 yılında Emniyet Genel Müdürlüğü bünyesinde İnternet ve Bilişim Suçları Şube Müdürlüğü görevlendirilmiş. 2004 yılında kanunla bilişim suçları düzenlenmiş ve 2005 yılında ceza kanunumuzda yer almıştır [9,10].

Kişisel verilerin korunması 1970 tarihli Almanya'nın Hessen Eyalet Veri Koruma Kanun ile yasalaştı [11]. Bilgi yönetiminde bilgi bütünlüğü önemlidir. Kişisel Verileri Koruma Kurumu'da veri ihlalleri ile ilgili şikayetleri değerlendirmektedir [12].

*Anayasamızla uyumlu Kişisel Verileri Koruma Kanununa göre veri sorumlusunun hakları şunla*rdır: Kişisel veri işlenip işlemediğini sorabilir. Buna ait bilgi talep edebilir. Bu verinin amacına uygun kullanılıp kullanılmadığını öğrenebilir. Üçüncü şahıslara veri aktarım durumunu isteyebilir. Eksik ya da yanlış veri işlenmesi halinde düzeltilmesini

isteyebilir. Aleyhine durum varsa düzelttirebilir. Zarar olmuşsa tazminini isteyebilir. Ceza Kanunu 136, 138'e göre ceza verilmesini talep edebilir. Buna göre siber güvenlik ilkeleri şunlardır: Risk yönetimine göre kabul edilebilir risk düzeyi uygun yöntemlerle sürekli sağlanır. Tehdit azaltılır. Paydaşların hukuki, idari, ekonomik, politik sosyal boyutlardaki farkındalığı sağlanır. Paydaşlar hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunmasına yönelik etkinliklere olumlu katkıda bulunur. Taraflar şeffaf, yenilikçi, hesap verilebilir ve etik değerlere uygun davranır. Risk için yakın orantılı ve gerçeklik özelliğine göre tedbir alınır [11]. COBIT ilkelerine göre Paydaş ihtiyaçları karşılanır. Kuruluşun uygulamaları baştan sona kapsar. Tek bir bütünleşik çerçeve uygulanır. Bütüncül yaklaşım sağlanır. Yönetişim yönetimden ayrıdır [11].

7.5. Veri Madenciliği

Tıp bilişimi biyomedikal alanda tanı ve tedavide vazgeçilmez unsurların arasında sayılmaktadır [13]. Maliyet/etkinlik artışı, kanıta dayalı tıp uygulamaları, hizmet üretimi artırılması, performans geliştirilmesi, tıpta uygulama hatalarının önlenmesi, azaltılması, tanınması, hasta memmuniyetinin artırılması ve eğitimi, güvenli hasta hekim ilişkisi ve SGK uygulamalarının izlenmesi açılarından faydalıdır [13, 14]. Olay yeri incelemelerinde bilişim teknikleri ile hukuki değerlendirmeler de geliştirilmiştir [15]. Tele sağlık, evde sağlık hizmetlerinin geliştirilmesi, robotik uygulamalar bilişimin vazgeçilmez konuları arasına girmiştir. Telefon teknolojisinde karşılaşılan ana bellek sorunlarının adli alanda çözümünde teknikler geliştirilmiştir [16].

Veriyle ilgili sınıflandırmada sıklıkla yararlanılan yöntemler şunlardır:

Denetimli: en yakın K komşuluk belirleme, K ortalamalar kümeleme, bayes sınıflandırıcı, regresyon modelleme, kural çıkarımı (arı modeli, karınca kolonisi, kuş sürüsü optimizasyonu, sürü optimizasyonu, parçacık sürü optimizasyonu, tabu araştırma, yapay bağışıklık, atıf, bulanık yöntem, sezgisel yöntem), karar ağaçları(analitik hiyerarşik model, kaba küme teorisi), yapay sinir ağları, genetik algoritma. Bilgi maksimizasyon modeli ile parmak izi gibi şekil tanıma durumları ile kimlik teşhisinin güvenilir saptandığı açıklanmıştır [17].

Denetimsiz: Aşamalı kümeleme, kendi kendini düzenleyen harita [18].

7.6. Sıklık ve Önem

Bilişim insan hayatının vazgeçilmezleri arasında sayılması yapay zekâ, derin öğrenme ile yaygınlaşmasındandır. Ulaşım ve devlet yönetim işlerinde siber saldırı demek görevlileri iş yapamaz hale sokmaktır. Şiir yazmak, film senaryosu oluşturmak, beste yapmak sıradanlaşmaktadır. Yapay zekânın yapamadığı ya da yapılamayan durumların da gerçekten yapılması gereken konular olup olmadığı da tartışılmaktadır.

7.7. Siber Suçlar

Bu suçlar beş başlık altında incelenebilir. Bunlar şunlardır:

1) Bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar (yasadışı erişim, virüs dağıtılması, sisteme müdahale, şirketlerin gizli bilgilerine ulaşılması, cihazların kötüye kullanılması): Kanunla Korunmuş bir yazılımın İzinsiz kullanılması Fikir ve Sanat Eserleri Kanunu'nda 'eser haklarına aykırıdır [19].
2) Bilgisayarlarla ilişkili suçlar (sanal sahtecilik ve sahtekarlık suçları): Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ile banka, kişisel v.s. gibi bilgilere yetkisiz şahıslar ulaşarak yarar sağlamaktadır [19]. Bilişim Yolu ile Nitelikli Dolandırıcılık TCK'nin m 158 aykırı fiildir. Banka Veya Kredi Kartlarının Kötüye Kullanılması (TCK m 244-245). Bilişim Sistemine Girmek: TCK 243'de; bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimse cezalandırılır. Ayrıca sigorta dolandırıcılığı, kara para aklama, bilgisayar sistemleri ve bilgisayar ağlarına girme, telefon dolandırıcılığı, üyelik abonelik dolandırıcılığı gözlenmiştir [20].

Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu: TCK 244'de; bir bilişim sisteminin işleyişini engelleyen cezalandırılır.

Bilişim yoluyla Hakaret, Sövme ve Şantaj TCK m 125'de yasaklanmıştır. Elektronik İmza Kanununa Muhalefet Borçlar Kanunu'nun 13. maddesine göre, sözleşmeye uymamaktır.

Bilişim Sistemleri Engelleme Bozma, Verileri Yok Etme veya Değiştirme durumu TCK m 244 e göre yasaklanmıştır [19]. Kişinin bu tür hatalı, hileli durumları anlaması için yapması gerekenler şunlardır:

- Başlık: İmla hatalarının olması, içerik uygunsuzluğu bulunması halinde web adresinin niteliği diğer web siteleri ile karşılaştırılarak doğruluğu kaydedilir.
- İnternet adresine (URL): URL adresinde küçük değişiklik veya hatalar bulunur. Gerçeği ile kıyaslanır.
- Kaynak: Gönderen kaynaktan bizzat sorgulanır.
- Yazı biçimi: İmla hataları, tuhaf-acayip, alışılmamış sayfa düzeni gözlenir.
- Fotoğraf: Fotoğraf taklit, değiştirilmiş, düzeltilmiştir.
- Tarih: Tarih ve yer düzenlemesi olguya özgü olmadığı gözlenir.
- Kanıt: Yazar uygunluğu, yazı içeriğinin akademik olmaması metnin geçerli ve güvenilir olmadığını gösterir. Diğer haber kaynakları ile uygunluk kıyaslaması yapılır. Kasıtlı yanlış bilgi paylaşılmaz.
- Yazı şaka, eğlence kasıtlı yazılmış olabilir.
- Bazı haberler kasten yanlış bilgi içerir.

3) İçerikle ilişkili suçlar (çocuk pornografisi suçu, hem sahip olmak hem de verilerin dağıtımını yapmak): İnsanlık onuru gereğince çocuk pornosu vb. yayınlar tartışma yürütmeksizin engellenmesi gereken içeriklerdir. İnsan özel yaşamını ihlal eden durumlar, sır niteliğindeki bilgiler hukuki sorunların başında yer alır [20]. Ticari sırların açıklanması, manyetik kartların şifrelerinin bozulması, bankamatik bilgilerinin çalınması ciddi sorunlardandır [21].
4) Fikri mülkiyet haklarının ihlali ile ilgili suçlar: 5651 Sayılı Kanunun 8. Maddesinin 1. Fıkrasında, erişimin engellenmesine konu olabilecek suçlar yer almaktadır (5651 Sayılı Kanun, 2007). Bu suçlar: 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nda (TCK) yer alan; 95-25/7/1951 tarihli ve 5816 sayılı "Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun"da yer alan suçlardır [22],
5) Suça yardım, teşebbüs ve teşvik etme suçları şunlardır:

- İntihara yönlendirme (TCK madde 84),
- Çocukların cinsel istismarı (madde 103, birinci fıkra),
- Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
- Sağlık için tehlikeli madde temini (madde 194),
- Müstehcenlik (madde 226): Müstehcenlik (TCK m 226)- İnternette Çocuk Pornografisi: Bu sitelerin % 60'ı ABD'de yapılmaktadır.
- Fuhuş (madde 227),
- Kumar oynanması için yer ve olanak sağlama (madde 228), [23-26].

7.8. Ülkemizde İnternet Üzerinden En Çok İşlenen Suç Tipleri

Kumar oynatılması yoluyla oynatan yüklü para kazanılmaktadır [27].

Hakaret içeren Atatürk ile ilgili YouTube videoları bulunmaktadır. Giderek artan çocuk pornografisi içeriğine, müstehcen içeriğe, intiharı körükleyen türden Satanist içerik ve websiteleri gözlenmektedir. Türk Ceza Kanunu'nun 226. Maddesine ve 5651 Sayılı Kanuna göre suçlar cezalandırılır. Bu nedenlerle bunlar üç grupta incelenebilir:

1) Kamusal çıkarların korunması için öngörülenler (ulusal güvenlik, ülke bütünlüğü, kamu güvenliği, suç ya da kargaşanın önlenmesi, ahlaki değerlerin veya sağlığın korunması),
2) Kişilik haklarını korumak için öngörülenler (itibarın veya başkalarının haklarının korunması, sır olarak edinilmiş bilgilerin gizliliğinin korunması),
3) Egemenliğin ve yargının tarafsızlığının korunması.

Çocuk pornografisi cinsel istismar öncüsüdür. İnsan ticareti yolunu açar [28]. Çocuk sömürüsü pornografi, fahişelik ve çocuk seks turizmi yoluyla yapılır. İnternet yoluyla çocuk köleleştirme arkadaşlık, bağlantı, risk değerlendirme, ayrıcalık oluşturma ve cinsel içerikli konuşmalarla basamakları ile yapılır [29]. Pedofili yaşça kayda değer büyük birinin çocuğu cinsel olarak tercih etmesidir.

Cinsel arzu açık konuşulur. Tuzak ile fikir paylaşılır. Seks felsefesi yapılır. Fail kimliğini saklar. Kolay ulaşılır ve izlenir [29]. Çocuk karaborsacılığı kişinin tehdit edilerek, güç kullanılarak (kaçırma), hileyle, yalanla, para ile, çıkar karşılığı toplanması, taşınması, iletilmesi, barındırılması, fatura edilerek sömürü amaçlı kontrol altında tutulmasıdır [29]. Çocuk ailesiyle bağlantısı koparılmaktadır. Kayıt dışı, ucuz, eğitim ve hak yoksunluğunda çalıştırılmakta. Terör üyesi yapılmaktadır. İnsan ticareti yapılır. Çocuğun cinsellikle ilgili sömürülmesinde çocuğun cinsel isteği ikinci planda ve pasif eş niteliğindedir. Seks objesi olarak tanımlanır. Baskı ortamı bulunur, güven ve samimiyet hisleri bulunmaz. İletişim dengeli değildir. TCK m 103 e göre pornografi müstehcenlik içinde sayılarak ceza ağırlaştırıcı etkenlerdendir. Bu alanda yaşanan sorunlar resim üzerinde yaş tayini yapılamaz. Görüntü sayı ve niteliği az oluşu, diğer görüntülerle karışması ve görüntü şifrelemesi ve/veya silinmesi nedeniyle zordur. TCK m 225 e göre pornografik içeriklerin yayınlanması ve saklanması yasaklanmıştır [28].Erişim Engelleme Kararlarının kaldırılması hukuka aykırı içeriği yayından kaldırmakla mümkündür.

Çöpe dalma, gizlice dinleme, veri aldatmacası, Truva atı, tarama, süper darbe, salam tekniği, gizli kapılar, eşzamansız saldırılar, ağ solucanları, bilgisayar virüsleri, sırtlama, mantık bombaları, istem dışı ileti alma, yerine geçme, kredi kartı sahtekarlığı ve diğer sorunlar olmak üzere yaygın ve farklı yöntemler kullanılmaktadır [30]. Sonuçta bilişim yoluyla devlete, halka, kişiye ait olmak üzere ceza kanununda belirtilen pek çok suçun işlenmesinde zemin hazırlanmaktadır [31,32].

Organize fiil: İkiden fazla kişinin işbirliği, işbölümü, devamlılık, kendine has bazı disiplin ya da kontrol sistemine sahip olma, ağır suçların işlendiğine ilişkin makul şüphelerin bulunması, uluslararası düzeyde faaliyetlerde bulunma, sindirmek amacıyla şiddet ya da uygun araçlar kullanma, ticari ve sistemli yapılar kullanma, para aklama faaliyetlerinde bulunma, politikacılar, medya, kamu yöneticileri, adli ya da ekonomik merciler üzerinde nüfuz kurmaya çalışma, etki ve güç elde etmeyi amaçlama şeklinde sıralanmaktadır [33,34]. Terörizm amatörleşme ve megaterörizm ile genişlemiştir. Dekapite ile liderin etkisizleştirilmesi, desantralize ile bulundukları yerin açıklanması ve güvensiz olduğunun vurgulanması ve deorga-

nizasyon ile bağlantı yollarının engellenmesi, ortadan kaldırılması gerekir [11].

6698 sayılı Veri Koruma Kanununa göre Sağlık Bakanlığı, sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve finansmanı amacıyla, elde edilen kişisel sağlık verilerini toplar ve istatistiki değerlendirir. Unutulma hakkı çerçevesinde verilerin silinmesi istenilebilir. Kişisel veriler bağımsız kurul tarafından korunur, denetlenir [33]. Ülkemizde, sağlık, cinsel hayat, biyometrik ve genetik veriler Kişisel Verilerin Korunması Hakkındaki Kanun kapsamında özel nitelikli veriler olarak tanımlanmıştır. Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği ile ilgili bilgiler korunmaktadır [35].

7.9. Kişinin Bilişim Aracılığı İle Bağımlı Olduğu, Kumar Oynadığı, Nefret Suçu İşlediği, Saplantılı Durum Geliştirdiği Durumlar

Bu durumlar aşağıda verilmiştir.

Gençler sıklıkla okul çağında yakınlarının başına bir şey gelmesi, önemli mesaj atlama, gelişmeleri kaçırma korkusu, eğlence, grup dışı kalma, tehlike haberi anlama, sosyal çıkıntı yapmamayı garantilemek, kaçamak yapmak ve ilişkide bulunulan kişiyi kızdırmamak, öfkelendirmemek amacıyla interneti sıklıkla kullanmaktadır. Ayrıca beğeni ve emoloji gibi unsurlarda işin içine girince duygu ve zaman bağımlı süreçler gelişmektedir [36,37]. Bağımlılık sebepleri aşağıda belirtilen modellerle ve teorilerle açıklanabilir:

1) Bilişsel davranış modeli: Ortamda stressiz, değerli olma hali kişinin başarı beklentisini artırır.
2) Öğrenme teorisi: Olumlu pekiştireç ödül ile kişi duygusal olumlu yüklenme geliştirir.
3) Genetik teori: Kişi yapısal olarak bağımlılığa elverişlidir.
4) Organik bozukluk: Beyinde belli odakların aktivite artışı söz konusudur.
5) Kayıp önleme modeline göre kişi kültürel etkileşimde bulunur.

Bu esnada rekabet çerçevesinde mükemmeliyete ulaşmak için bilişim teknolojik uygulamaları daha sık izler. Bu sosyal öğrenme ile kontrol geliştirir. Günah keçisi kavramına göre kendisini suçlar, utanır. Diğerini ötekileştirir. Kontrol kaybı artar. Yetersiz sosyal beceri vardır.

6) Ödül eksikliği: Bağımlılığın dikkat çekme, duygu durum değişikliği, internette geçirdiği zamana tolerans, internetsiz durumda huzursuzluk, endişelenme tarzı geri çekilme belirtileri, çatışma ile öfke nöbetleri yoksunluk belirtisi olarak bilinir. Nüks ile benzer davranışların pekiştirilmesi ve yeniden düzenleme özellikleri bulunur [38-40]. Sosyal ilişkileri bozulur. İş hayatı bozulur veya okul başarısı düşer. Aile ilişkileri zayıflar. Tekrar bağlantı için her türlü sıkıntıya girer [36].

7) İnternet Bağımlılık kriterleri şunlardır:

- İnternet ile ilgili aşırı zihinsel uğraş ve dikkat çekme
- İnternete bağlı kalma süresinde artışa ihtiyaç duyma ve mutlu olma
- İnternet kullanımını azaltmaya yönelik başarısız girişimlerde bulunma
- İnternet kullanımının azaltılması durumunda yoksunluk belirtileri
- Başlangıçta olduğundan daha uzun süre internete bağlı kalma
- İnternettin aşırı kullanılması yüzünden ilişkiler, okul ya da işle ilgili sorunlar yaşama
- İnternete bağlı kalabilmek için aile üyelerine, terapiste veya başkalarına yalan söyleme
- İnternete bağlı kalındığı süre içerisinde duygulanım değişikliğinin olması (mutluluk, ödül alma, umutsuzluk, suçluluk, anksiyete, depresyon gibi).
- Belirtiler psikotik bozukluk, bipolar bozukluk ile açıklanamaz
- Üç aydan fazla sürer [40].

8) Tedavi

Psikoterapi olarak bilişsel, davranışçı tedavi, aile tedavisi, destek tedavisi uygulanır. Psikiyatrist ilaç olarak antidepresan, duygu-

durum düzeltici, anksiyolitikleri önerebilir [41]. İletişim kurmayan ve tedavide çok zorlanılan kişiye kanuni müşavir veya vasi atanması için mahkemeye başvurulabilir.

9) Kumar oynama bozukluğu: Kumar oynama davranışı daha yüksek bir kazanç elde etmek umuduyla başka bir şeyi riske atmaktır. Sonunda kişisel, ailevi ve sosyal sorunlar yoğunluk kazanmaktadır. Bu kişilerde anksiyete, depresyon gibi hastalıklar sıktır. Hastalığın ruminatif karakteri ve dürtüsel tutumla olan birlikteliğini tedavi planlamasında göz önünde bulundurularak bütüncül yaklaşım gerekmektedir [42].

10) Nefret ve ayrımcılık suçu: Irk, etnik köken, cinsiyet, din gibi sebeplere dayanarak, kişilere haksız fiil yapılmasıdır. TCK m 122 ye göre suçtur. TCK 216 maddesine göre de kamu güvenliğini tehlikeye sokma suçu da işlenebilir. Önyargı esastır. İletişim yoluyla saldırı sonucu mağdurda toplusal ilişkilerde zayıflık, öfke ağırlıklı yoğun duygular, üzüntü, öğrenme sorunları, mesleki bütünlük ve benlik duygusunu zedelenmesi, kişinin kendine yönelik kuşkusunu artması, paranoya'ya ve kafa karışıklığı, güven duygusunu yitirilmesi, mağdur kendisini yalıtması, huzursuzluk, korku, utanç, öfke, endişe gözlenir. Önleme ve tedavi: İtiraz edilir. Açıklanır. Eğitim yapılır.

11) Saplantılı durumu: Bilişim alanındaki verilerle iz sürme, takip mümkündür. Bu yolla kişi karşılıksız aşık olduğu kişiyi izler. Onunla ilgili bilgiler yayar, kurtuluş olmadığında yaralama, öldürme ve malına zarar verme suçlarını işler.

İzhar: Sahtekarlık, hırsızlık, yolsuzluk gibi iddia edilen bir suçu; ırk, din, milliyet, cinsiyet vb. ayrımcılığı veya misillemeyi; bir yasaya, bir düzenlemeye, bir devlet politikasına, ahlaki değerlere, etik kurallara veya terbiyeye aykırı oluşumu; toplumun sağlığını ve güvenliğini tehlikeye sokan hususları açığa çıkartmak ve/veya şikayet etmek amacıyla yapılan, bir kamu kuruluşundaki ya da özel sektördeki bir kişiyle, kurumla veya örgütle yapılan sözlü veya yazılı iletişim izharcılık olarak bilinir. İzharcı, resmi ya da gayri resmi kanalları kullanırken kendisi hakkında bilgi vermekten kaçınmayıp her türlü sorumluluğu kabullenebilmekte ya da izharcılığın sonuçlarından korkup endişeye kapılarak; izharcılık eylemini isimsiz mektuplar, isimsiz telefonlar ve kişisel bilgi içermeyen elektronik

posta ve web siteleri aracılığıyla gerçekleştirip, izharcılık süreci boyunca anonim kalmayı tercih edebilmektedir [43]. Kurum kültürünü olumsuz etkileyerek tükenmişliğe, yıldırıya, işten ayrılmaya, performans düşmesine, intihar veya cinayete yol açtığından hukuk dışı uygulamalardan kaçınılması, korunulması, önlenmesi, ortadan kaldırılması gerekir.

Kişi ölümcül hastalığı, akıl hastalığı, başarısızlığı gibi nedenlerle ölmek isteyebilir. Bu durumda yardımlı ölüme ötenazi denilmekte. Bizzat zehiri sağlayarak, ölme yolunu göstererek aktif ötenazi, ölme yolunu açıklayarak, tedavi yapılmasını sağlamayarak pasif ötenazi yapılmasına vesile olunabilir. Ölmek isteyenin istemine göre de istemli veya istemsiz ötenazi yapılabilir. Aktif ötenazi durumu onurlu yaşam hakkı gerekçesiyle acıma duygusuyla uygulanması halinde kasten insan öldürme suçu (TCK m 81,82) işlenir. Pasif ötenazi ise başkasının intihara azmettiren, teşvik eden, intihar kararını kuvvetlendiren kişi intihara yardım (TCK m 84), görevini yapmaması halinde ihmal suretiyle insan öldürmeye (TCK m 83) nedeniyle cezalandırılır. İnsanı yaşatma yönünde davranış geliştirme vatandaşlık görevidir. Ceza, tazminat davası açılabilir [37].

7.10. Değerlendirmeler

Her etkinlik kaydedilir. Kayıt dışı durumlarda yetkililer bilgilendirilir. Yasa dışı durumda gizlilik esas olduğundan çocuk hayır demesi öğretilir ve yardım isteme gereği, eğitimin sürme gereği açıklanır ve sağlanır. Çalışma hayatında iş sağlığı ve güvenliği ilkeleri esastır. İş sağlığı ve güvenliği tedbiri alınmış. İş yeri hekimi ilk muayene ve periyodik muayene yapmaktadır. Sosyal bağlantılar kuvvetlendirilir.

Rehabilitasyon programları uygulanır. Failler cezalandırılır. Uluslararası eşgüdüm bağlantısı ile süreç izlenerek tedbir alınır. Medya aracılığı ile toplum bilgilendirilerek yeni olgu açığa çıkması önlenir. İzlem dışı olgu varsa kayda geçilerek gereken yapılır [44]. Konu ağ haritalama ile bulanık mantık ilkeleri ile önemlilik, öncelik açısından tanımlanır, çözüm üretilir. Dinamik güvenlik kurallarına göre olumlu davranışı teşvik edilir [45]. İş Sağlığı ve Güvenliği alanında ilk muayene, periyodik muayene gerekir. Çocuk hafif iş yapabilir. Eğitimde geçirdiği süre çalışma süresindendir. Anne baba velayet hakkının kötüye kullanılmamasını sağlar. Eğitimciler çocuğun çalışması halinde ihbar eder.

Sendika aracılığıyla çocuk üstün yararı korunur [46]. Koordineli çocuk işçiliği önleyen durumlar yaygınlaştırılır [47].

İfade özgürlüğü, unutulma hakkını engellemesi halinde sınırlama yapılması "sansür çerçevesinde değerlendirilmemeli, özel hayata saygı çerçevesinde düşünülmesi gerekir [46].

Bilgi güncel, sade, kolay iletilebilir, önemli, öncelikli durumu belli, nesnel gerçeğe uygun sunulmalıdır. Konu olaya ilintili yakın elverişli ve orantılı sunulmuş olup neden-sonuç bağlantılıdır. Cümle kavramsal anlamı, yan anlamı, çağrışımsal anlamı, toplumsal anlamı, duygu değeri, yansıma anlamı, eşdizimsel anlamı ve konusal anlamı açısından bütünsellik içerir. Kelimeler alt anlam, eşanlam, karşıt anlam, eşsesli ve çok anlamlılık, eğretileme, parça bütün ilişkisi ve ad eksiltilmesi açısından içeriğe uygundur [49,50]. Bilimsel tıbbi yazılar sistematiktir, tıp teknolojisi ve terminolojisi, alan çalışması açısından denetlenmiştir. Kanıta dayalı tıp içeriği bulunur. Sınırlılık ve önyargılar tanımlanmıştır. Epidemiyolojik veriler standardizedir. Kanıt değeri ve önemi güçlü olup, atıf yapılabilir, impact faktörü yüksek dergide yayınlanmıştır. Plasebo etki belirgin ayrıktır. Gereksiz tedavi ve hasta suistimali önlenmiştir. Yarar/zarar oranı yüksek ve anlamlı önceliklidir. Tamamlayıcı tıp uygulamaları desteklenmiştir. Tıp uygulamalarına alternatif değildir [51-52].

Ağ güvenliği için IPSec (Internet Protokol Security), WEP (Wireless Equivalent Privacy), WPA (Wireless Proteced Access), RSN (Robust Security Network), ESP (Encapsulated Security Payload), AHP (Authentication Header) protokolleri sık kullanılmaktadır. Ayrıca güvenlik düzeyini artırmak için güvenlik duvarı, IKE (Internet Key Exchange) gibi farklı yöntemlerde kullanılmaktadır. VPN (Virtual Private Network)'de internet üzerinden ağlara kontrollü olarak IP tüneli ile bağlanmayı sağlamaktadır [53]. Hata veritabanı madenciliğinde; hata düzeltme sürecini doğru kişiye atamak, tekrarlı hata raporlarını bulmak ve raporlanmış bir hataya doğru ağırlık değeri atamak gerekir [54]. Bundan hata yönetiminde yararlanıldığı düşünülmüştür [55].

Bilirkişilik alanında disiplinlerarası, işbirliğine dayanan, bilgi dokumante edilen, standart uygulanan ve hata denetimine elverişli olan sistem üretme ve çalışmasını yürütme yükümlülüğümüz ve sorumluluğumuz bulunmaktadır.

Kaynaklar

[1] http://www.ankarabarosu.org.tr/Siteler/1940-2010/Kitaplar/pdf/a/aihm50.pdf (ET 15.01.2017).

[2] https://ekitap.alternatifbilisim.org/files/yeni_medya_calismalari-1_kongre_kitabi.pdf (ET:15.01.2017).

[3] Özen M, Özocak G. Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134). *Ankara Barosu Dergisi*, 2015, 1:1-38. http://dergipark.gov.tr/download/article-file/398234 (ET 16.05.2018).

[4] Özbek M. Adli bilişim uygulamalarında orijinal delil üzerindeki hash sorunları. Ist International Symposium on digital forensics and security 20-21 May 2013, Elazığ. http://www.bilgisayardedektifi.com/wp-content/uploads/2013/06/MuratOZBEK_Adli_Bilisimde_Orijinal_Delil_Uzerindeki_hash_Sorunlari_isdfs_bildiri.pdf (ET 18.05.2018).

[5] Bilge Y. Ankara Üniversitesinde bilirkişilik. https://www.researchgate.net%2Fprofile%2FYasar_Bilge%2Fpublication%2F235434066_Dava_Acma_Sebepleri%2Flinks%2F57a43c2408aee07544b15702%2FDava-Acma-Sebepleri&usg=AOvVaw2DkomJH-Kd8EjvgcMvQSXg (ET 01.06.2018).

[6] Şirikçi AS, Cantürk N. Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının(İmaj Almak) Önemi. Bilişim Teknolojileri Dergisi 2012:5/3; 29-34.

[7] Vincze, Eva A. Challenges in digital forensics. Police Practice and Research 2016:17/2: 183-194.

[8] Gündüz TK. Adli Bilişimde Delil Güvenliği: Mevcut Sorunlar, Çözüm Önerileri. *Turkiye Klinikleri Journal of Forensic Medicine-Special Topics*, 2017: *3*(3), 141-145.

[9] Şamlı R. Türk ve dünya hukukunda bilişim suçları. Akademik bilişim'10-XII. Akademik Bilişim Konferansı Bildirileri s 1-7, 10-12 Şubat 2010, Muğla.

[10] Dülger MV. Karşılaştırmalı hukuk bağlamında birleşik krallık (İngiltere) hkukunda bilişim suçları mevzuatı ve uygulaması. Türkiye Adalet Akademisi Dergisi 2017:31:141-257.

[11] Efe A. Bilişim hukuku ile uluslararası hukuk kesişiminde yeni bir paradigma. "Siber Yönetişim. Türkiye Noterler Birliği Hukuk Dergisi 2017/2:157-206, 2017.

[12] Kişisel Verileri Koruma Kurumu. https://www.kvkk.gov.tr/Icerik/2051/Ozel-Nitelikli-Kisisel-Veriler (ET 01.06.2018).

[13] Demirhan A, Güler İ. Bilişim ve sağlık. Bilişim Teknolojileri Dergisi 2011:4/3:13-20.

[14] Bilge Y. Türkiye Klinikleri Adli Tıp Özel Dergisi "İnsan Sağlığını Tehdit Eden Terör Suçları Özel Sayısı" (Cilt:1 Sayı:2): http://www.turkiyeklinikleri.com/journal/adli-tip-ozel-dergisi-e-dergi/2149-3804/

[15] Lars CE, Tuan TN, Breitbeck R, Marcel B, Michael JT, Ross S. The forensic holodeck: An immersive display for forensic crime scene reconstructions. Forensic Sci Med Pathol 2014:10;623-626.

[16] Yang SJ, Choi JH, Kim KB, Bhatia R, Saltaformaggio B, Xu D. Live acquisition of main memory data from Android smartphones and smartwatches. Digital investigation 2017:23:53-62.

[17] Busey T, Nikolov D, Chen Y, Emerick B, Vanderkolk J. Characterizing Human Expertise Using Computational Metrics of Feature Diagnosticity in a Pattern Matching Task Cognitive Science 2017: 41/7:1716-1759.

[18] Gönül Y, Ulu Ş, Bucak A, Bili A. Yapay sinir ağları ve klinik kullanımı. Genel Tıp Derg 2015;25:104-111.

[19] Koç, S., & Kaynak, S. (2010). Bilişim suçları bağlamında yeni medya olarak internet ve kişisel güvenlik. *Akademik Bilişim Konferansı 2010*. S 1-43.

[20] Silahtaroğlu G. Veri madenciliği. Kavram ve algoritmaları. Papatya Yayıncılık Eğitim s 15, İstanbul, 2016.

[21] Altunok E, Vural AF. Bilişim suçları. 2011/8. dergipark.gov.tr/download/article-file/208853. (ET 18.05.2018).

[22] Yıldız S. (2010), Kitle İletişim Mevzuatı, Nobel Yayınları: Ankara s 224-225.

[23] Eryılmaz Mehmet (2014), Türkiye ve Dünya'da İnternet Erişiminin Engellenmesi İle İlgili Düzenlemeler, Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü: Afyonkarahisar.

[24] Yıldız S (2006), Suçta Araç Olan İnternetin Teknik ve Hukuki Yönden İncelenmesi, Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü: Konya 161.

[25] Şenormancı, Ö. (2012). Internet Addiction: Pharmacological and Cognitive Behavioral Therapy of Online Gaming, Sex, Gambling and Shopping. *Bulletin of Clinical Psychopharmacology*, *22*(1), S13.

[26] Yıldız S. (2013), Medya ve Hukuk (3. Baskı), Nobel Yayınları: Ankara.

[27] Ocak A. Hakları dengelemek: Unutulma hakkı ifade özgürlüğüne karşı. TAAD 2018: 9/33507-535.

[28] http://www.cyber-rights.org/reports/internet_yasak_siyah.pdf (ET 15.01.2018).

[29] Polat O. Çocuk pornografisi. Nokta Kitap, 2007, İstanbul.

[30] Dokurer S, Bilişim suçları laboratuarlarında çocuk pronografisi incelemeleri. http://dokurer.net/files/documents/ChildpornExamining.pdf ET 16.05.2018.

[31] Hekim H, Başıbüyük O. Siber suçlar ve Türkiye'nin siber güvenlik politikaları. Uluslar arası Güvenlik ve Terörizm Dergisi 2013:4/2;135-159.

[32] Kuloğlu G. Organize suç istihbaratı operasyon yönetimi ve bir model önerisi. Polis Bilimleri Dergisi 2012:14/4:1-30.

[33] http://www.tasam.org/Files/PDF/Raporlar/avrupa_birligi_istihbarat_kurumlari__68fd6a58-a9f4-4dbb-bc7e-02ab691a6572.pdf (ET 19.05.2018).

[34] Büken NÖ, Ünsal ÇZ. Kişisel verilerin korunması kanununun biyomedikal alana yansımaları açısından değerlendirilmesi. Hacettepe HFD 2017:7/2;33-54.

[35] http://www.tdk.gov.tr/ (ET 24.05.2018).

[36] Dale CF, Fontana VC, Martinez JA. What's your vice? A combined aproach to drugs and other addictive substances and activities. Addiction Research and Theory 2016: 24/5:366-374.

[37] Eroğlu A, Bayraktar S. İnternet bağımlılığı ile ilişkili değişkenlerin incelenmesi. *International Journal of Social Sciences and Education Research 2017: 3*(1), 184-199.

[38] Çetinkaya L, Sütçü, S. Çocukların gözüyle ebeveynlerinin bilişim teknolojileri kullanımlarına yönelik kısıtlamaları ve nedenleri. *Turkish Online Journal of Qualitative Inquiry*, 2016: *7*(1), 79-116.

[39] http://www.turkdilbilgisi.com/sozcukte-anlam/gercek-yan-mecaz-anlamli-sozcukler.html (ET 24.05.2018).

[40] http://www.tdk.gov.tr/ (ET 24.05.2018).

[41] Griffiths, M., & Barnes, A. (2008). Internet gambling: An online empirical study among student gamblers. *International Journal of Mental Health and Addiction*, *6*(2), 194-204.

[42] Taş F, Antalyalı ÖL. Kamu Hastanelerinde ve özel Hastanelerde çalışan Hemşirelerin izharcılık (whistleblowing) tutumları. MAKÜ İktisadi ve Ticari Bilimler Fakültesi Dergisi 2015:2/2/3; 34-54.

[43] Bilge Y, Ruhsal Değer Sisteminde seçim zamanı. Öncü Kitabevi, 2014.

[44] Altıntaş, M . (2018). Kumar oynama bozukluğu tanısı olan hastalarda, anksiyete, depresyon, ruminasyon ve dürtüsellik. Cukurova Medical Journal, 43 (3), 624-633. DOI: 10.17826/cumj.356820.

[45] Haydar E, UluoğluSA. Dünyada çocuk işçiliğiyle mücadelede gelinen nokta ve geleceğe dair bazı öngörüler. *Eğitim Bilim Toplum* 13.51 (2015): 46-72.

[46] Görücü, İ, Akbıyık N. (2010). Türkiye'de Mevsimlik Tarım İşçiliği: Sorunları Ve Çözüm Önerileri/Seasonal Agricultural Workers in Türkiye: Their Problems and Solution (Proposal) s. *Hikmet Yurdu*, *3*(5), 189-220.

[47] Tahiroglu AY, Çelik GG., Fettahoglu Ç, Yıldırım V, Toros, F, Avcı A, Özatalay E, Uzel, M. (2010). Psikiyatrik Bozukluğu Olan ve Olmayan Ergenlerde Problemli Internet Kullanımı.Nöro Psikiyatri Arşivi Dergisi 47(3), 241.

[48] Bozkurt H, Şahin S, Zoroğlu S. İnternet bağımlılığı: Güncel bir gözden geçirme. Journal of Contemporary Medicine 2016:6/3;235-247.

[49] Warmerdam L, Straten AV, Twisk J, Cuijpers P. Predicting outcome of internet-based treatment for depressive symtoms. Psychotherapy Research 2013:23/5:559-567.

[50] Bilge Y, Adli Tıp Kitabı, Üçüncü baskı, İstanbul Tıp Kitabevi, 2013.

[51] Gürler C. Nefret suçları ve iş hayatı. http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2010-1/2010-1-gurler.pdf (ET 30.05.2018).

[52] Polat HH. Halk hekimliği ve tamamlayıcı alternatif tıp üzerine bir değerlendirme. Toplum ve Hekim 2017: 32/1:29-37.

[53] Karakurt1 HB, Koçak C , Doğru İA. Kablosuz Ağlarda Çok Katmanlı Güvenlik ve Performansa Etkisi. Karaelmas Fen ve Müh. Derg. 8(1):126-137, 2018.

[54] Bilgin TT, Gökhan A. "Yazılım hata logları kullanılarak veri madenciliği uygulaması gerçekleştirilmesi." *Marmara Fen Bilimleri Dergisi* 27.1 (2015): 14-20

[55] Li WF, Chen HC, Nunamaker, JF. Identifying and Profiling Key Sellers in Cyber Carding Community: AZ Secure Text Mining System. Journal of Management Information Systems 2016: 33/4: 1059-1086.

Siber Güvenlikte Sigortalama

BÖLÜM 8

Gürol CANBEK

SİBER GÜVENLİKTE SİGORTALAMA

Geleneksel sigorta anlayışının siber uzayda izdüşümü olarak kabul edeceğimiz siber sigorta gerek sigorta anlayışındaki deneyimlerimiz gerekse zeminin siber uzay olması ile yanlış değerlendirmelere yol açabilecek bu konudur. Bu bölümde siber sigortanın, geleneksel sigorta ile de bağlantılarına temas ederek ne tür bir tedbir olduğu ele alınmaktadır.

8.1. Giriş

Son zamanlarda ülkemizde ticarinin yanında bireysel siber güvenlik paketleri ile gerek kurumları gerekse kişileri "siber suçlardan korur" şeklinde takdim edilen siber sigortanın, doğru bir şekilde anlaşılması ve çok disiplinli, karmaşık bir boyut olarak siber güvenliğin sigortacılık ile etkin ve verimli bir şekilde etkileşimi mühim bir konu olarak karşımıza çıkmaktadır.

"Siber sigorta: başlı başına etkili bir çözüm olabilir mi?"

Siber sigorta, özellikle ağ tabanlı kullanıcıların siber uzayda karşılaşacakları risklerin sigorta primi olarak adlandırılan belirli bir meblağ karşılığında bir sigorta şirketine aktarılmasını sağlayan bir risk yönetim tekniğidir. İnternet hizmet sağlayıcılar, bulut sağlayıcılar (veri merkezleri) ve çevrimiçi hizmet sunan ya da hassas bilgileri işleyen banka gibi kurumlar olası siber sigorta müşterileri arasında yer almaktadır.

Hemen bir pencere açmak adına belirtmek gerekirse; siber sigortanın yararına inananlar, siber sigortanın, sigortacılar tarafından uygun seviyede "öz savunma güvenilirliğini" (garantisi değil) müşterilere yönlendiren sigorta sözleşmeleri tasarlamaya ilettiğini ve bu şekilde siber uzayın daha güçleneceği düşünmektedir.

Öz savunma, başta kurumsal olmak üzere ağ tabanlı BT kullanıcılarının, sistemlerini, geleneksel savunma hattının akla gelen ilk

tedbirleri olan virüs koruma ve sağanak kovar yazılımlar, güvenlik duvarları ve güvenli işletim sistemlerinin kullanımı gibi teknik çözümler ile bu sistemleri güvenli kılmak için sergiledikleri çabalar anlamına gelmektedir.

8.2. Öz (Siber) Savunma

Gittikçe sayısallaşan her türlü altyapı, bilgisayar ağları üzerinden sunulan hizmetler ve kullanıcıların bizzat kendisi; dağıtık hizmet aksattırma saldırısı, kimlik hırsızlığı gibi çeşitli saldırı girişimleri, gizli dinleme, bilişim korsanlığı, sazan avlama, bilgisayar solucanları, virüsler, ileti sağanakları gibi tehditler tarafından ortaya konulan geniş çeşitlilikte risklere maruzdur.

Bu tehditler tarafından oluşturulan risklere karşı koymak için kullanıcılar, geleneksel olarak tehditlerden etkilenme olasılığını düşüren, virüs koruma ve sağanak önleme yazılımları, güvenlik duvarları, saldırı tespit sistemleri ve diğer siber savunma unsurlarına başvurmaktadır. Bu yaklaşımın sürdürülebilirliği açısından, büyük bir güvenlik sanayii (örneğin büyük virüs koruma şirketleri) ticari faaliyetleri ve özellikle akademik bakış açısıyla gerçekleşen kayda değer AR-GE çabaları; hali hazırda siber altyapı ve kullanıcılarını, tehditlerin ve kasıtlı/kasıtsız anormalliklerin neticesinde ortaya çıkan olumsuz etkilerden korumak için bu tehdit ve anormallikleri tespit eden ve dahası önleyen araçlar ve teknikler geliştirmeye ve bu unsurları kendi bilgi varlıkları etrafında konuşlandırmaya odaklanmaktadır.

Dolayısıyla, öz savunma hem kullanıcıya sunulan tedbirler hem de kullanıcının bu tedbirleri kendisine en uygun şekilde uyarlaması ile mümkün olmaktadır.

8.3. Siber Sigortanın Ortaya Çıkışı: Öz Savunmada Mükemmel Siber Güvenlik Yanılgısı

Geliştirilen donanım, yazılım ve kriptografik yöntemler neticesinde son on beş yılda risk hafifletme tekniklerindeki ilerlemelere rağmen, mükemmel ve hatta mükemmele yakın siber güvenliğin başarıldığını düşünmek bir yanılgıdan öteye gitmemektedir.

Mükemmel siber güvenliğin imkânsızlığı [1], özellikle siber sigortacılık çerçevesinde, aşağıda çeşitli kaynaklardan derlenen bir sıra nedenden kaynaklanmaktadır:

- Sağlam teknik çözümlerin kıtlığı,
- Ağ saldırılarının gerçekte arkasında yatan niyetleri ayırt edip, hedef alacak çözümlerin tasarlanmasındaki zorluk,
- Ağın korunması ile ilgili; yöneticiler, kullanıcılar, güvenlik ürünü satıcıları ve yasal düzenleme organları arasında çelişen beklenti ve odaklar,

Diğer kullanıcıların güvenlikteki yatırımları nedeniyle ortaya çıkan olumlu güvenliğin etkilerinden yararlanan kullanıcıların, sonrasında güvenliğe yatırım yapmaması sebebiyle ortaya çıkan "**bedava biniş" (***free-riding) sorunu,*

*Müşterinin harekete geçememesi ve korunmasız güvenlik ürünlerinin "***ilk hareket eden etkileri",**

- Etkin ve yerinde risk hafifletme çözümlerinin tasarımı ile ilgili aşılması güç noktaların ortaya çıkardığı gecikme,
- Güvenlik üreticilerinin pazarda güçlü ürünler çıkarabilmek için teşviklere sahip olmaması nedeniyle "**kötü iyiyi kovar" sorunu**[1],
- Ürün satıcıları tarafından oynanan "**güvenilirlik aldatmacası oyunu" (***bul karayı al parayı),*
- *Teknik çözümlerin özelliklerinin yararlarından en uygun şekilde faydalanılmasındaki "***kullanıcı toyluğu".**

Yukarıda sıralanan sebepler ve risklerin çeşitliliği karşısında siber uzayda risk yönetimi için daha farklı seçenekler değerlendirilmeye alınmıştır. Bu durum, ABD Başkanı Obama'nın 2013 yılında siber tehditlerin azaltılması ve bu tehditlere karşı esnek olunmasına vurgu yapan güvenlik tasarısında, siber sigortanın etkin risk yönetimi için henüz farkına varılmayan bir araç olarak tanımlanması ile ifade edilmiştir. Bugün geldiğimiz noktada siber sigorta, bir siber saldırı olayında son savunma hattı unsuru olarak değerlendirilmektedir.

1 **Limon pazarı sorunu (***lemons market); 1970'lerde Ekonomist Ekerlof'un makalesinde yer alan, satıcı ve alıcılardaki* **bilgi asimetrisi nedeniyle "***limonların" (ABD'de kusurlu olduğu satın alındıktan sonra anlaşılan 2. el arabalar için kullanılan tabir) "şeftalilerin" (yüksek kaliteli 2. el arabaları) önüne geçmesi.* **Ters seçim (***adverse selection) olarak da tanımlanmaktadır.*

8.4. Siber Sigorta Teminatları

Siber sigorta, işletmeleri ve bireysel kullanıcıları İnternet tabanlı risklerden ve daha genel olarak, BT altyapısı ve faaliyetleri ile ilgili risklerden korumak için kullanılan nispeten yeni bir sigorta ürünüdür. Daha önceleri siber uzaydaki bu riskler, genel olarak geleneksel ticari genel yükümlülük poliçelerinde hariç tutulur veya en azından geleneksel sigorta ürünlerinde belirgin bir şekilde tanımlanmazlardı.

8.4.1. Siber Sigortada Birinci Taraf Teminat, Yükümlülük Teminatı ve Diğer Kapsanan Konular

Siber sigorta poliçelerince arz edilen teminat kapsamı genellikle şunları içermektedir:

- Veri tahribatı, gaspı, hırsızlığı, bilişim korsanlığı ve hizmet aksattırma saldırıları gibi kayıplara karşı **birinci taraf teminat** (first-party coverage)
- Hatalar ve ihmal neticesinde verinin korunamaması veya karalama ya da itibar kaybı (defamation) gibi başkalarına karşı kayıplar için firmaları tazmin eden **yükümlülük teminatı** (liability coverage)
- Düzenli güvenlik denetimleri, siber olay sonrası halkla ilişkiler, soruşturma masrafları ve gerçekleşen bilişim suçu ile ilgili ödül koyma fonları.

8.4.2. Birinci Taraf Teminat ve Maliyetleri

Birinci taraf teminat kapsamı ve bu kapsam ile ilgili olabilecek maliyetler genelde şunları içerir [2]:

- **Adli bilişim soruşturması:** Veri gediği şüphesinde atılacak ilk adımlar, gediğin oluşup oluşmadığına karar vermek ve sonrasında gediğin sebep ve kapsamını soruşturmaktır. Bu kapsamın karşılanması için bir adli bilişim bilirkişisi tutmak gerekebilir.
- **Bilgisayar ve veri kaybının yerine koyulması ve yeniden kurulması:** Bilişim korsanlığı neticesinde zarar gören masa ve dizüstü bilgisayarlar, sunucuların yerine konulması ve veriler ile ilgili kayıpların iyileştirilmesi için gereken işlemler.

- **İş kesintisi ve ilave faaliyetler:** Birçok işletme için bilişim sistemlerinin devre dışı kalması para kaybı anlamına gelmekte ve bu nedenle başvurulabilecek başka bir ağ hizmetinin tahsis edilmesi ve ihlâle müdahale eden çalışanların fazla mesai yapması gibi noktalarda ortaya çıkacak maliyetler dikkate alınır.
- **Halkla ilişkiler:** Veri gedikleri, özellikle mali, teknolojik, ulaşım ve sağlık iş kollarında müşteri kaybına sebep olmaktadır. Bu tür bir ihlâl durumunda; müşteriler, iş ortakları ve kamuoyu ile uygun bir şekilde iletişim kurulması gerekmektedir. Bu çerçevede halkla ilişkiler danışmanları, basın ve avukatlar ile beraber çalışabilir.
- **Bildirim, çağrı merkezi ve kredi izleme:** ABD'de üç eyalet haricinde 47 eyalette, kişisel bilgilerin bulunduğu güvenlik ihlâllerinde bu ihlâllerden etkilenen bireylere de bildirim yapılması zorunluluğu bulunmaktadır (Bknz. Güvenlik Gediği Bildirim Yasası). Türkiye'de Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Madde 6'da haberleşme iş kolunda buna benzer bir bildirim yükümlülüğü bulunmaktadır. Bu maksatla bir çağrı merkezinin görevlendirilmesi ve bazı eyaletlerde resmi merciler dışında ayrıca kredi izleme kurumlarına bu konuda bildirim yapılması gerekebilmektedir.
- **Elektronik hırsızlık ve dolandırıcılık koruması:** Yaşanan olaylar ele alındığında; suçluların, sadece hasara yol açmak için veya veri toplamak için değil, özellikle para çalmak için sistemlere saldırmaya kalkıştığı ortaya çıkmaktadır. Bu kapsam, bu tür hadiseler sonucunda oluşan mali kayıpları karşılar.
- **Siber gasp:** Son yıllarda, özellikle fidye yazılımlar ile yapılan, verilerin kullanıcı bilgisayarları içinde şifrelenmesi ve bu şifrenin kaldırılması için kurbandan para istenmesi gibi vakalar ile karşılaşılmaktadır. Bu tür durumlarda yapılacak bir şey olmayınca, fidye talebinin suçluya verilmesi gerekebilir (Bknz. ABD polisinin kilitlenen dosyalarını açmaları için fidyeyi ödediği örnek bir vaka: [3]).

8.4.3. Siber Sigortanın Gerçekçi Faydaları

Ülkemizde bugünlerde yaşandığı gibi, birçok ülkede siber sigorta pazarı, diğer sigorta ürünlerine göre daha yeni ve nispeten ve şim-

dilik küçük çaplı olduğundan, siber sigortanın ortaya çıkabilecek siber tehditler bakımından etraflıca etkisini ölçmek tek başına bir vaka bile ele alındığında zordur. Ancak; siber tehditlerin, insanlara ve işletmelere etkisi, sigorta ürünlerinin sağladığı koruma kapsamına nazaran daha da genişlemeye devam ettikçe, sigorta şirketleri, hizmetlerini geliştirmeye devam edeceği öngörülebilir. Sigortacılar, siber saldırılar nedeniyle ortaya çıkan kayıpları karşıladıkça ve tehditler de gelişip değiştikçe; var olan BT güvenlik hizmetleri ile beraber sigorta ürünleri de artan şekilde satın alınmaya başlayacaktır.

Ancak, günümüz koşulları değerlendirildiğinde, siber sigortacılığın ne kadar olgun olduğu noktasında önemli şüpheler gözükmektedir. Öncelikle, sigortacılar açısından siber sigorta ürünleri önerebilmek için gereken **poliçe yazma** (underwriting) kıstasları, konunun karmaşıklığı ve deneyimli uzman açığı nedeniyle gelişiminin erken safhalarındadır. Bu yüzden, **poliçe yazıcıların** ürünlerini daha da geliştirmek için BT güvenlik şirketleri ile etkin bir şekilde ortaklık kurması en tabii yaklaşımdır.

8.4.4. Temel Faydalar

Kişisel verilerin korunması kanunu ile güncel bir konu haline gelen sayısal mahremiyet sigortacılık açısından değerlendirilmesi gereken başlıca konular arasında yer almaktadır. Öncelikle, geleneksel yükümlülük poliçelerinin özellikle kişisel bilgilerin toplandığı işler için önemli bir fayda getirmediği bilinmektedir [4]. Siber sigortanın bu noktada kayda değer katkılarının olabileceği temel güdü açısından göz önünde bulundurulmalıdır.

Temel bakış açısıyla; siber sigortanın, güvenliği geliştirmeye doğrudan katkısı yanında; büyük çaplı bir güvenlik hadisesinde oldukça önemli katkılar sunabilmektedir.

Genel olarak siber sigorta,

- Büyük çaplı zararlardan geri dönmede,
- İşlerin normale döndürülmesinde ve
- Devlet desteğine olan ihtiyacın azaltılmasında

daha "pürüzsüz" bir fonlama mekanizması sağlamaktadır.

8.4.5. Siber Risklerin Adil Dağılımı: Risk - Prim

Siber sigorta özünde; siber risklerin, bu tür risklerden beklenen kaybın daha çok olduğu şirketler için daha yüksek prim ile adil bir şekilde dağılmasına olanak verir.

Bu **bedava binişi** (free-riding) hem de riskin potansiyel olarak tehlikeli bir şekilde toplanmasını önler. Siber sigorta, aslında siber sigortacıların, tüzel ve özel kullanıcıların, poliçe yapıcıların ve güvenlik yazılımı üreticilerinin ekonomik teşvikler ile hizalanabilen bir pazar çözümü haline gelme yeterliliğine sahiptir.

Daha ayrıntılı ele alınacak olursa;

- Siber sigortacılar, primlerin uygun bir şekilde fiyatlandırılması ile kâr elde edebilirler;
- Ağ tabanlı kullanıcılar hem sigorta satın alarak hem de öz savunma yöntemlerine yatırım yaparak maruz kalabilecekleri kayıpları kısıtlamaya çalışırlar;
- Poliçe yapıcılar, güvenlik piyasasının ideali olan "uçtan uca ağ güvenliğinde" ilerlemeye önemli katkı sağlayabilirler ve
- Güvenlik yazılımı üreticileri, siber sigortacılar ile iş birliği yaparak ürün satışlarında artış sağlayabilirler.

Siber sigortanın faydalarının sıralandığı bu noktada beklentileri gerçekçi kılmak adına siber sigortanın ne olduğunun dışında siber sigortanın ne olmadığı da değinilmesi gereken bir husustur.

8.5. Siber Sigorta Ne Değildir?

Konut sigortaları nasıl deprem, yangın veya hırsızlığı engellemiyorsa; siber sigorta da ihlâllerin oluşmasını engelleyemez. Kaçınılmaz olarak sigortalılar, sigortacıların belirttikleri güvenlik gereksinimleri karşılamaktan çok; işleri için en uygun olan kontrolleri seçtikleri ve uyguladıklarından emin olmaları gerekir. Bu yüzden temel "mühim kontrollerin" tamamıyla ve sürekli izlenir şekilde uygulanması yerinde olacaktır.

Bu noktada başta kullanıcılar olmak üzere tüm paydaşlar farkında olunması gereken bir nokta da siber sigorta ile geleneksel sigorta arasındaki farkın ne olduğudur. Geleneksel sigortacılığın karşılaya

geldiği risklerin yanında siber riskler farklı bir niteliğe sahiptir. Başta mobil teknolojiler olmak üzere gittikçe yaygınlaşan ve her paydaş tarafından temel seviyede anlaşılması güç olan siber güvenlik ele alındığında [5]; birbirine bağımlı ve ilintili karmaşık bir tabiatta olan riskler, siber sigortaya hastır. Geleneksel sigorta senaryolarından (örneğin araç veya sağlık sigortası) çok daha farklı boyuta ve parametreye bağlıdır. İnternet gibi uçsuz bucaksız dağıtık bir sistemlerin sisteminde gerçekleşebilecek riskler, kavranabilmesi ve öngörülebilmesi çok güç bir yayılıma sahiptir ve farklı farklı riskler birbirleriyle ilintilidir. Geleneksel sigortada yayılım çoğunlukla bir bazen de iki ya da biraz daha fazla varlığa yayılım gösterir.

Herkes evinin önünü süpürürse…

Bu bakımdan, güvenlik üzerindeki risklere karşı koymak için siber sigortanın tetiklediği her türlü kullanıcı yatırımı ve oluşturulan yaklaşımlar, aslında İnternet üzerindeki diğer kullanıcılar için dışsallık (externality) olarak ifade edilen olumlu kazanımlar doğurmaktadır. Burada siber sigortanın amacı; bireysel kullanıcıların ağdaki dışsallıkları içselleştirmesini sağlamak ve böylelikle her bir kullanıcının en uygun şekilde güvenlik çözümlerine yatırım yapması sağlayıp ahlaki tehlikenin hafifletilmesine ve başta İnternet dâhilinde olmak üzere topyekûn siber güvenliğinin gelişmesine imkân vermektir. Ancak, bu yaklaşım dışsallıkların kullanıcı yatırımı ile çok daha kolay içselleştirildiği geleneksel sigortalara göre biraz daha güç ve zahmetlidir.

8.6. Dünyada Siber Sigorta Pazarının Gelişim Tarihçesi

Siber sigortanın mevcut durumunun anlaşılması açısından gerçekleşen gelişmelere göz atmak yerinde olacaktır. 1990'lı yıllara gelindiğinde siber sigortanın ilk gelişimine yol açan adımlar açısından dağıtık bilgisayar sistemlerinde risklerin konumlandırılmaya çalışıldığı ve e-ticaret gibi uygulamalarda yer alan sigorta protokollerinden istifade edildiği görülmüştür. Bilgi güvenliğinin iş hayatında öneminin hissedildiği 2000'li yıllarda siber sigortanın temel risk yönetim aracı olduğu en azından bir gelecek hedefi olarak dile getirilmeye başlanmıştır.

Tam da bu dönemde siber sigorta pazarı, 2000 yılı sorununun doğru bir şekilde ele alınmaması ve 11 Eylül saldırısının getirdiği odak kaybı ile olması gereken ilerlemesini gerçekleştirememiştir. Günümüze gelindiğinde uç noktada değerlendirilen oyuk bir enstrüman olarak değerlendirildi. Ancak, en tutucu tahminlerde bile küresel siber güvenlik pazarının çok büyük boyutlarda olacağı ifade edilse de İnternet ekonomisinde yaşanan büyümeye nazaran siber sigorta pazarı yeterince büyüyememiştir.

Siber sigorta pazarı, 2010'dan itibaren yükselişe geçmiş ve 2015 çoğu ABD olmak üzere küresel olarak 2 milyar ABD doları prim satışı gerçekleşmiştir [6].

İlk Kuşak Siber Sigorta (2005 ve öncesi)

Yukarıda ifade edildiği gibi uygulamada yaşanan bazı engeller ve siber güvenliğin baş etmesi gereken ciddi tehditlere odaklanması nedeniyle 2005 yılına kadar siber sigorta pazarının belirli bir olgunluğa eriştiği söylenemez.

İlk kuşak şeklinde tanımlanan dönemde ortaya çıkan temel engeller şu şekilde dile getirilmiştir:

- Sigorta primlerini hesaplamak için gereken sigorta istatistikleri ile ilgili (aktüeryal) verinin eksikliği,
- Karar verici mercilerdeki pazarda ancak çok küçük talebe dönüşen farkındalık eksikliği ve
- Yasal ve prosedürel engeller.

Örneğin; yasal ve prosedürel engeller, hasar telâfi taleplerinde hayal kırıklığına neden olduğundan siber sigortanın yayılması mümkün olmamıştır. Belki ülkemizde şu dönemde yaşanan bir konu olarak, sigorta yapmayı düşünen tüzel kişiliklerin, BT altyapılarını ve politikalarını açık eden bir dizi güvenlik değerlendirme prosedürlerinden geçmesi gerekliliği müşterileri bu noktada çekimser bir duruma sokmuştur.

Ancak, bu dönem ve sonrasında yaşanan çok sayıda saldırıya, güvenlik en iyi uygulamaları, standartlarında ve adli bilişim yaklaşımlarında gerçekleşen gelişmelere rağmen dünyanın gelişmiş ülkelerinde bile tesis edilmiş bir sigorta pazarının kurulamaması ayrıca değerlendirilecek bir konudur.

Fakat, bu konuda bazı görüşleri kısaca dile getirmek, özellikle ülkemizde hayat bulmaya başlayan siber güvenlik pazarının doğru bir şekilde konumlandırılması açısından önemli olabilir. Uzmanlara göre siber sigortada beklenen gelişmenin olamaması; sigortacılar-sigortalı-bağımlılar olarak adlandırılan üç sac ayağı arasındaki risk bilgisi asimetrisi ile açıklanmaktadır.

Bu asimetrinin özellikle,

- Farklı türlerde (düşük ve yüksek riskli) kullanıcılar arasındaki farkı ayırt etmede yetersizlik (ters seçim sorunu) ve
- Kullanıcıların sigorta sözleşmesi imzalandıktan sonra zarar görme olasılıklarını kötü yönde etkileyecek eylemlere girişmesi (ahlaki tehlike)

ile meydana geldiği ifade edilmektedir.

8.7. Türkiye'de Siber Sigorta için Yasal Dayanaklar

Aşağıda siber sigorta kapsamında değerlendirilmesi gereken yasal düzenlemeler listelenmiştir:

T.C. Anayasası

20. Madde: A. Özel Hayatın Gizliliği

Herkes, özel l ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. **Özel hayatın ve aile hayatının gizliliğine** dokunulamaz.

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; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

Türk Medeni Kanunu (Tertip 5, 11.07.2013)

B. Kişiliğin korunması. II. Saldırıya karşı. 1. İlke. Madde 24

- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

- Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.

(Kişilik hakkı: Yaşam, sağlık, özgürlükler, şeref ve haysiyet, özel yaşam, isim, resim, his yaşamı gibi kişisel varlıklar üzerindeki haklar [1])

Türk Borçlar Kanunu (Kanun No: 6098)

IV. İşçinin kişiliğinin korunması. Madde 417

İşverenin yukarıdaki hükümler dâhil, kanuna ve sözleşmeye aykırı davranışı nedeniyle işçinin ölümü, vücut bütünlüğünün zedelenmesi veya kişilik haklarının ihlaline bağlı zararların tazmini, sözleşmeye aykırılıktan doğan sorumluluk hükümlerine tabidir.

İş Kanunu (Tertip 4, 11.09.2014)

İşçi özlük dosyası. Madde 75

- İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır.

- İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve **gizli kalmasında işçinin haklı çıkarı bulunan bilgileri** açıklamamakla yükümlüdür.

Yetkili memurların ödevi. Madde 93

İş hayatını izleme, denetleme ve teftiş yetkisi olan iş müfettişleri görevlerini yaparlarken işin normal gidişini ve işyerinin işlemesini, inceledikleri konunun niteliğine göre mümkün olduğu kadar aksatmamak, durdurmamak ve güçleştirmemekle ve resmi işlemlerin yürütülüp sonuçlandırılması için, açıklanması gerekmedikçe, işverenin ve işyerinin meslek sırları ve şartları, ekonomik ve ticari hal ve durumları hakkında gördükleri ve öğrendikleri hususları **tamamen gizli tutmak** ve kendileri tarafından bilgileri ve ifadeleri alınan yahut kendilerine başvuran veya ihbarda bulunan işçilerin ve başka kişilerin isimlerini ve kimliklerini açıklamamakla yükümlüdürler.

Türk Ceza Kanunu (Tertip 5, 04.04.2015)

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.

(2) Kişiler arasındaki **haberleşme içeriklerini hukuka aykırı olarak ifşa** eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini **diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi**, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (Ek cümle: 2/7/2012-6352/79 md.) İfşa edilen bu **verilerin basın ve yayın yoluyla** yayımlanması halinde de aynı cezaya hükmolunur.

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) (Değişik: 2/7/2012-6352/80 md.) 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.

Özel hayatın gizliliğini ihlal. 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.

(2) (Değişik: 2/7/2012-6352/81 md.) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu **verilerin basın ve yayın yoluyla yayımlanması** halinde de aynı cezaya hükmolunur.

Kişisel verilerin kaydedilmesi. Madde 135

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

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin **bilgileri kişisel veri olarak kaydeden** kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

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.

Nitelikli haller. Madde 137

(1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve **görevinin verdiği yetki kötüye kullanılmak** suretiyle,

b) **Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak** suretiyle,

İşlenmesi halinde, verilecek ceza yarı oranında artırılır.

Verileri yok etmeme. Madde 138

(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

(2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.

Şikâyet. Madde 139

(1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikâyete bağlıdır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması. Madde 140

(1) Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik (5 Kasım 2011 ve 29 Ocak 2013 [Madde 4: 6 ve 7. fıkra ve Madde 9: 2. fıkrada değişiklik])

Destek Hizmeti Alınması. Destek hizmetine ilişkin sınırlamalar. Madde 4.

(6) Başka şirket bünyesinde istihdam edilen personel, 1 inci maddenin ikinci fıkrasının (a) bendinde sayılan işlerde, çağrı merkezi, müşteri ziyareti şeklinde yapılanlar dâhil pazarlama, veri girişi, dosyalama, arşiv, yönetici asistanlığı, bankanın idari işlerinin takibi, bilgi sistemleri gibi hizmet alanlarında, bankada geçici veya sürekli olarak çalıştırılabilir. **Bu kapsamdaki personele verilecek sisteme erişim, veriye erişim veya veriyi görme yetkisi işin gerektirdiği bilgiyi kapsayacak şekilde sınırlandırılmalıdır**.

Destek hizmeti kuruluşlarında aranacak şartlar. Sözleşmenin unsurları. Madde 7

d) Destek hizmeti kuruluşu tarafından sağlanan hizmet dolayısıyla öğrenilen **bankalara ve müşterilerine ait bilgi ve belgelerin güvenliğinin sağlanmasının** zorunlu olduğu hususunun belirtilmesi,

Destek hizmeti kuruluşlarının denetimi. Madde 9.

(1) Kurum, destek hizmeti kuruluşlarından Kanun ve bu Yönetmelik hükümleri ile ilgili göreceği bütün bilgileri gizli dahi olsa istemeye, tüm defter, kayıt ve belgelerini incelemeye yetkili olup, destek hizmeti kuruluşları da istenilen bilgileri vermekle, sistem, süreç, defter, kayıt ve belgeleri incelemeye hazır bulundurmakla, tüm bilgi işlem sistemini denetim amaçlarına uygun olarak Kurumun yerinde denetim yapan meslek personeline açmakla, **verilerin güvenliğini sağlamakla** ve muhafaza etmek zorunda oldukları her türlü defter, belge ve karneler ile vermek zorunda bulundukları bilgilere ilişkin elektronik, manyetik ve benzeri ortamlardaki kayıtlarını ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifrelerini inceleme için ibraz etmek ve işletmekle yükümlüdür.

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik (24 Temmuz 2012, Sayı: 28363)

Kişisel verilerin işlenmesine ilişkin ilkeler. Madde 4

(4) (Ek:RG-11/7/2013-28704) İşletmeci tarafından yetkilendirilen taraflarca bu Yönetmelik hükümlerinin ihlal edilmesi de dâhil olmak üzere **kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının** temininden işletmeci sorumludur.

Güvenlik. Madde 5

(1) İşletmeciler, kişisel verilerin işlenmesine ilişkin olarak **güvenlik politikası belirler**. İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin **güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri** alır. Söz konusu güvenlik tedbirleri, teknolojik imkânlar göz önünde bulundurularak **muhtemel riske uygun bir düzeyde** sağlanır.

(2) Birinci fıkrada belirtilen tedbirler, asgari istem dışı, yetki dışı ya da yasa dışı olarak; **kişisel verilerin tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesine karşı kişisel verilerin korunmasını** içerir.

(3) (Değişik: RG-11/7/2013-28704) İşletmeciler, **kişisel verilere sadece yetkili kişiler tarafından erişilebilmesini ve kişisel verilerin saklandığı sistemlerin ve kişisel verilere erişim sağlamak için kullanılan uygulamaların güvenliğini sağlamakla** yükümlüdür.

(4) (Değişik: RG-11/7/2013-28704) İşletmeciler, kişisel verilere ve ilişkili diğer sistemlere yapılan **erişimlere ilişkin işlem kayıtlarını saklamakla** yükümlüdür.

(5) (Değişik: RG-11/7/2013-28704) Kurum, gerekli gördüğü hallerde işletmecilerden, **kişisel verilerin saklandığı sistemlere ve alınan güvenlik tedbirlerine ilişkin tüm bilgi ve belgeleri isteme, ayrıca söz konusu güvenlik tedbirlerinde değişiklik talep etme** hakkını haizdir.

Riskin ve kişisel veri ihlalinin bildirilmesi. Madde 6

(1) (Değişik: RG-11/7/2013-28704) İşletmeci, şebekenin ve kişisel verilerin güvenliğini ihlal eden belirli bir risk olması durumunda bu risk hakkında Kurumu ve Kurum tarafından gerekli görülmesi halinde abonelerini/kullanıcılarını etkin ve hızlı bir şekilde bilgilendirmekle yükümlüdür.

(2) Bu riskin işletmeci tarafından alınan tedbirlerin dışında kalması halinde, söz konusu riskin kapsamı, giderilme yöntemleri ve yaklaşık maliyeti hakkında abonelerin/ kullanıcıların etkin ve hızlı bir şekilde bilgilendirilmesi sağlanır.

(3) İşletmeci, kişisel veri ihlali olması durumunda söz konusu ihlalin niteliği ve sonuçları hakkında abonelere/kullanıcılara yapılacak bilgilendirmenin detayları ve ihlalin giderilmesi için alınan tedbirlere ilişkin olarak Kurumu bilgilendirir.

(4) Kişisel veri ihlalinden abonelerin/kullanıcıların olumsuz yönde etkilenme ihtimalinin bulunması halinde işletmeci, kişisel veri ihlalinin niteliğine, daha fazla bilginin elde edilebileceği iletişim noktalarına ve ihlalin olası olumsuz etkilerini azaltmak için aboneler/kullanıcılar tarafından alınabilecek önlemlere ilişkin olarak aboneleri/kullanıcıları ücretsiz olarak bilgilendirir.

(5) İşletmeci, gerçekleşen kişisel veri ihlallerine ilişkin olarak söz konusu ihlalin sebeplerini, etkilerini ve çözüme yönelik tedbirleri içeren bilgileri gizliliğini ve bütünlüğünü sağlayarak kaydetmekle yükümlüdür.

Tıbbi Deontoloji Tüzüğü (12 Ocak 2015)

Madde 4

Tabip ve diş tabibi, meslek ve sanatının icrası vesilesiyle **muttali olduğu sırları, kanuni mecburiyet olmadıkça, ifşa edemez**.

Hasta Hakları Yönetmeliği (1 Ağustos 1998, Sayı: 23420)

Bilgilerin gizli tutulması. Madde 23

Sağlık hizmetinin verilmesi sebebiyle edinilen **bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz**.

Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın **hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi**, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir.

Araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın açıklanamaz.

Kişisel Verilerin Korunması Kanunu

Tamamı dikkate alınmalıdır.

8.8. Değerlendirmeler

Bu bölümde siber güvenlikte nispeten yeni bir ufuk açan ve ülkemizde de yeşermeye başlayan siber sigorta konusu ele alınmıştır. Siber sigortanın, başta kurumsal ve nihayetinde kişisel kullanıcıları kapsayacak şekilde etkin bir öz savunma getirmede önemli bir tetikleyici etken olduğu değerlendirilmiş; ancak bu savunmanın mükemmel siber güvenlik yanılgısına neden olmayacak şekilde gerçekçi bir şekilde algılanması ve ele alınması gerekliliği ortaya konulmuş; siber sigortanın temel yönleri açıklanmış; siber sigorta ile ilgili gerek geleneksel sigortacılık gerekse siber sigorta gelişiminde ortaya çıkan olumsuz noktalar özetlenmiş ve ülkemizde siber sigortacılığın gelişiminde ciddi bir şekilde ele alınması ve farkında olunması gereken yasal düzenlemeler derlenmiştir.

Kaynaklar

[1] G. Canbek, "Siber savaşın eşiğinde: sıfırıncı gün {On the verge of cyber war: zero day}," *Aljazeera Turk*, 2015.

[2] W. C. Wagner, "Cyber Insurance: What do Cyber Insurance Policies Cover and Cost?," *Privacy & Data Security Insight*, 2015.

[3] N. Brinkerhoff, "Illinois and Massachusetts Police Pay Bitcoin Ransom to Hackers," *AllGov*, 2015.

[4] W. C. Wagner, "Cyber Insurance: Why You Need It If Your Organization Collects Consumer Data," *Privacy & Data Security Insight*, 2015.

[5] G. Canbek, "Cyber Security by a New Analogy: 'The Allegory of the "Mobile" Cave,'" *J. Appl. Secur. Res.*, vol. 13, no. 1, pp. 63–88, 2018.

[6] E. Nakashima, "Insurance requirements can drive stronger cybersecurity, Treasury official says," *Washington Post*, 2015.

Siber Güvenlik İçin Siber Yönetişim

BÖLÜM 9

Dr. Ahmet EFE - Prof. Dr. Türksel KAYA BENSGHIR

SİBER GÜVENLİK İÇİN SİBER YÖNETİŞİM

Siber alandaki tehditlerin giderek karmaşıklaşması, derinleşmesi ve yaygınlaşması karşısında meydana gelen hak ihlalleri, bireysel ve kurumsal hak ve özgürlük alanlarının çok ötesine geçtiğinden dolayı, uluslararası siber operasyonlar artık sadece bilişim hukukunu değil, uluslararası hukuk alanında çalışan akademisyen ve uygulamacıların da doğrudan doğruya ilgi alanına girmektedir. Artık siber tehditler ve siber terör olayları karşısında bireyler, firmalar, kurumlar ve devletlerin hak ve egemenliklerini koruyacak yeni hukuksal mekanizmalar ve uygulamalar geliştirilmektedir. Ancak, bilişim teknolojisi ve üretilen zararlı yazılım ve teknikler paralelinde değişen hukuki normlar ve mevzuat ile uygulamaya konulan stratejilerin, birbirileriyle uyum içerisinde olmaması ve ilgili paydaşların da etkin iletişim ve yönetişim içerisinde kararları al(a)mamaları, siber tehditlerle mücadelede kaynakların israf edilebilmesine, giderek hakim aktörlerin hegemonyasına girilmesine ve gerekli önlemlerin etkin ve verimli olarak alınamamasına neden olmaktadır. Bu çalışmamız, barış halindeyken siber alandaki uluslararası hukuk ve hak ihlalleri bilişim hukuku kapsamında ulusal sorumluluğunu irdelemekte ve ulusal siber güvenlik stratejisi kapsamında yönetişim paradigmasıyla teknik, idari ve stratejik çözümler aramaktadır. Çalışmamızda, Bilgi Toplumu Stratejisi, E-Devlet Stratejisi ve Siber Güvenlik Stratejileri arsında bir ahenk ve uyum olabilmesi için "Siber Yönetişim" kavramının bilişim hukuku, uluslararası hukuk ve kamu yönetimi disiplinlerinin kesişiminde ortak bir terminoloji olarak konumlandırılabileceği savunulmaktadır. Bu maksatla, kamu sektöründe yönetişim, stratejik yönetim ve kalite anlayışının uluslararası standartlar çerçevesinde oturtulması gerektiği ortaya konularak, ulusal siber güvenlik stratejisinin başarılı olabilmesi için ilgili paydaşların ahenk içerisinde uygulanması gereken yöntem ve alınması gereken tedbirler araştırılmaktadır. Kı-

sacası, siber güvenlik ile ilgili stratejilerin başarılı olabilmesi için yönetim ve yönetişim gereklilikleri ile ulusal ve uluslararası hukuki sorumlulukları teknik uygulamalarla birlikte ele alarak kurumsal ve ulusal ölçekte kaynak, değer ve risk optimizasyonunu sağlayacak bir çerçeve standardın benimsenmesi gerektiği ve özellikle COBIT çerçevesinin bu anlamda bütünlükçü ve paydaş ihtiyaçlarına dayanan modeliyle ihtiyacı karşılayabilecek nitelikte olduğu görülmektedir. Çok disiplinli bir yöntemle yapılan analizler sonucunda siber yönetişim için bir model önerisi geliştirilmiştir.

9.1. Giriş

"*Bu tamamen veri ile ilgilidir*" şeklindeki yaklaşımın bir gereği olarak, tüm sistem ve altyapının veri üzerine. "*Her şey aslında veri bütünlüğü ile ilgilidir*" şeklindeki bir yaklaşım aslında daha doğru olabilir. Verinin korunması siber güvenliğin, mahremiyetin ve işleyen internetin merkezinde olsa da aslında çoğumuz verinin işlenmesiyle elde edilen enformasyonun son kullanıcılarıyız. Bu nedenle de bazı araştırmacılar siber yönetişime yaklaşırken veri güvenliğine ek olarak enformasyon bütünlüğüne daha fazla önem verilmesi gerektiğini savunmuşlardır [33]. Ancak sadece verinin bütünlüğü değil, gizliliği ve mevcudiyeti ve denetim izi de siber yönetişim kapsamında dikkate alınması gereken hususlardandır.

Bir ağlar ağı olarak İnternet, onu kontrol etmek için merkezi ve güdümlü bir otoriteye sahip değildir. Benzersiz bir isim ve numara tanımlayıcıları atamak için merkezi bir otorite ihtiyacını kabul ederek, Alan Adı Sistemi 1980'lerin başlarında geliştirilmiştir. Birçok İnternet öncüsü ve İnternet özgürlüğünü destekleyenler, bu benzersiz tanımlayıcıların atanmasının tek gerekli internet yönetişim işlevi olduğunu savunurlar. Bununla birlikte, kötü amaçlı yazılım, artan kimlik hırsızlığı, mali suç, internetin terörist amaçlarla kullanımı, kurumsal casuslukların benzeri görülmemiş seviyeleri ve devlet aktörleri tarafından saldırıya açık siber savaş ve siber sömürü kabiliyetlerinin gelişmesi, daha güçlü ve daha geniş kapsamlı bir yönetişimin olabileceğini gösteriyor.

İnternetin büyümesi, küresel ticarete değer katmaya devam etmesi, ticaretin giderek internet ortamına taşınması ve milyarlarca günlük hayatı zenginleştirmesi için gerekli olması bu alanın zafiyetlerini,

kırılganlıklarını ve tehditlerini de arttırmaktadır. Artan siber suç maliyetleri, sanayi casusluğunun ekonomik tehdidi ve siber uzlaşmanın askeri nitelikler de taşıması göz önüne alındığında, "laissez-faire" olan liberal yaklaşımı artık sürdürülemez hale getirebilmektedir. Bugünün interneti, hükümet, özel sektör ve akademik toplumun işbirlikçi çabalarının ürünü olmakla birlikte, tarihsel haklar, İnternet'in geleceğini kontrol altına almıyor. Hükümet, güvenlik sorunlarının çözümü için gerekli olan liderliği sağlamada başarısız olursa, uluslararası kurumlar devreye girecektir. Facebook ve ABD seçimlerinde siber müdahale ve suiistimal gibi durumlar giderek yaygınlaşma eğilimi göstermektedir. Siber yönetişimde sadece uluslararası kurumlar, devletler ve mesleki örgütler dışında firmaların da farklılaşan rolleri olmalıdır. Çünkü elektronik ortamda elde edilen kazanç arttığı gibi bu alanda kitleleri etkileme ve kolay müdahale giderek artış eğilimi göstermektedir.

Siber yönetişim rejimi, en iyi şekilde birbirine kenetlenen uluslararası anlaşmalar, stratejiler, yasalar, önlemler, düzenlemeler ve standartlar düzeneği olarak anlaşılabilir. Bu parçalar birlikte veri koruma, kritik altyapı, şifreleme, internet içeriğini geliştirme ve koruma yanında BT endüstrisinin çıkarlarını destekleme kurallarını da kapsamak durumundadır.

Siber güvenlik konusunun bilişim hukuku ile uluslararası hukuk bağlamında değerlendirmesini yapmak, sorun tespit etmek ve önlemler serisi geliştirebilmek için öncelikle konunun teknik boyutunun ne olduğu ve ne tür risklerin mevcut olduğunun detaylı bir şekilde ortaya konulması gereklidir. Sorun ve riskleri azaltmaya, hak ihlallerinin meydana gelmesini önlemeye ve sürdürülebilir esnek sistemler geliştirmeye yönelik yasal, idari ve adli düzenlemeler ve uygulamalar da bilişim hukukunun çerçevesini teşkil etmektedir. Bilişim hukuku da siber yönetişimi ve uluslararası aktörleri dikkate almak durumundadır.

Siber saldırılar, veri ve enformasyon hırsızlığı, fidye saldırıları ve finansal yolsuzluğu içerebilir. Daha da ötesinde organizeli siber suçlar endüstriyel kontrol sistemlerini ele geçirme, yönetim ve kontrol verilerini toplama sistemlerini tahrip etmeyi de hedefleyebilmektedir. Fiziksel olarak çok iyi korunan ve yerin altında olan İran Nük-

leer zenginleştirme üniteleri Stuxnet olarak bilinen bir saldırıya maruz kalarak sistemin bozularak programın ciddi bir şekilde aksatılmasında görüldüğü gibi artık İleri Düzey Kalıcı Saldırılar (APT) ile fiziksel olarak yapılması çok zor veya imkânsız olan tahribatın sanal ortamda kolayca yapılabildiği anlaşılmıştır.

Askeri ve ticari sektör, e-devlet hizmetleri, enerji üretim ve dağıtım sistemleri de gene siber saldırılara maruz kalabilmekte ve ulusal açıdan çok büyük zararlar meydana getirilebilmektedir. Bu nedenle de ulusal ölçekte bir siber strateji ile tüm kurumlar tarafından alınabilecek önlemler sistematize edilerek yönetilebilir hale getirilmeye çalışılmak durumundadır. Ancak strateji oluşturulması, uygulanması ve raporlanması da iyi bir yönetişim mekanizmasının işletilebilmesiyle başarılı olabilir. Geçmişteki ulusal stratejilerin amacına uluşmaması bunun en önemli gerekçesini teşkil etmektedir. Aksi durumda ihtiyaç olmayan veya kaynak israfına yol açabilecek önlemler alınırken, kritik ve hassas risklerin ihmal edilmesi ve kontrol altına alınamaması da söz konusu olabilir.

Siber alan, 21. Yüzyılda artık sadece kişisel ve sosyal değil, siyasal, askeri ve ekonomik ilişkilere de nüfuz etmektedir. Artık modern toplumların dayandığı kritik altyapıların bütüncül bir parçası haline gelmiş ve iletişim şekilleri ve sosyalleşme biçimlerini kökünden değiştirmiştir. Siber alanda yönetişim, dolayısıyla uluşan ve küresel yönetişimin ayrılmaz bir parçası haline gelmiş ve diğer alanlarda etkin yönetişim için uygulanabilecek ortak hareket modellerinin test edildiği bir zemin sunmaktadır [3].

Burada cevaplanması gereken en önemli iki soru kuşkusuz *"siber alanı kim yönetmeli ve nasıl?"* olarak karşımıza çıkmaktadır. Bu soru ulusların siyasal ve ekonomik bağımsızlığını da ilgilendirmektedir. Sorulara cevap verebilmek için öncelikle farklı yönetişim modellerinin incelenerek sürecin geliştirilmesi için önerilerde bulunulması gerekmektedir. Bunlar da karar alma süreçlerinde daha fazla şeffaflığın sağlanması, dezavantajlı kesimlerin güçlendirilmesi ve bilinçlendirilmesi için finansal kaynak ayrılması ve adil bir şekilde uygulama yapabilecek liderlik pozisyonlarını belirlemek olarak tespit edilebilir. Ancak siber alanın küresel aktörleri, her tarafı bağlayıcı ve uygulanabilir ulusal ve uluslararası hukuksal zemini, ulusları,

ulusüstü organizasyonları ve kontrol altına alınamayan pek çok parametreyi barındırdığı için geleneksel yönetim ve yönetişim biçimleri ile başa çıkılacak bir durum söz konusu olmamaktadır. Bu nedenle siber yönetişim paradigması ön plana çıkmak durumundadır.

9.2. Siber Alanda "Yönetişim" Eksikliği

Yapılan literatür taraması sonucuna göre, bilişim hukuku alanında pek çok sorunun mevcut olduğu tespit edilmiştir. Bunlardan başlıcaları; Elektronik verilerin ticarileştirilmesinde sorun yaşanması, arama motorlarının sorumluluğu ve internet hukukunda problemler, internet sansür ağının oluşumuyla ilgili sorunlar, sosyal medya aracılığıyla işlenen suçların artması, yeni nesil akran zorbalığı-siber zorbalığın artması, bilişim ortamındaki kişisel bilgileri koruyamamak, mahremiyetin ihlali ve yetkisiz erişimler, siber suçun tanımı ve içeriği hakkında henüz bir uzlaşı sağlanmamış olması ve klasik ceza hukukunun yetersiz kalması, internetin yaygınlaşması ile birlikte ülkeler arasında fiziki sınırların belirlediği klasik hukuk anlayışı yetersiz kalması, bilgi kaynaklarına uzaktan erişim, fikri mülkiyet, kullanıcı gizliliği ve bilgi bütünlüğünün sağlanması konularında henüz bilişim dünyasındaki etik kurallar üzerinde uzlaşının sağlanmamış olması, E-imzanın teknik, uygulama ve mevzuat altyapısının yetersiz olması, Türkiye'de bulut bilişim kullanıcılarının veri güvenliğini ve gizliliğini yeterli seviyede koruyan bir hukuksal düzenlemenin bulunmaması, adli bilişimin bağımsız bir bilimsel disiplin alanı olarak henüz gelişimini sağlayamamış olması, Türkiye'de gerçekleşen birçok İnternet sitesi erişime engelleme kararı telif hakkı ihlaline dayandığından dolayı sanal ortamdaki hak ihlallerinin engellenememesi, teknoloji ve internet aracılığıyla para aklama ve terörizmin finansmanı gibi suçlarda bu sistemleri kullanan kara para aklayıcıların yüksek miktarda işlem yapabilmesinden dolayı ayrıca da yine hızlı bir şekilde de para miktarlarını istedikleri şekilde ayarlayabiliyor olmasının önlenememesi ve her türlü hak ihlallerine yol açan uluslararası siber operasyonları engelleyememek olarak ifade edilebilmektedir [16, 17].

Yukarıda verilen araştırmalar, bilişim hukuku kapsamında pek çok analiz ve değerlendirme yapıldığını ortaya koymaktadır. Kamu idareleri tarafından hazırlanan stratejiler de bu alandaki sorunların çözümlenmesine yönelik bir takım eylem ve faaliyetleri içerebilmektedir. Ancak, teknik bilgi ile birlikte kurumsal, ulusal ve bireysel

sorumluluklar açısından uluslararası ve bilişim hukuku boyutlarının birlikte ele alınarak analiz ve çözümleme yapılması noktasında ciddi bir araştırma eksikliği olduğu anlaşılmıştır.

"Siber yönetişim" kavramı ile ilgili olarak Türkçe alanyazında her hangi bir çalışma olmadığı dikkate alındığında bu kavramın alanyazına (literatüre) tanıtılması noktasında çalışmamızın akademik katkısının önemli olduğu düşünülmektedir. Türkçe literatürde bu noktada dikkate alınabilecek bir yayın EBSCO veri tabanı taramasında da tespit edilememiştir. Bu nedenle de bu çalışmamızda teknik ve hukuki alanda yapılmış çalışmalarla ilgili literatür taraması yapılarak buralarda ele alınmış olan sorunlar ile çözüm önerilerinin uluslararası hukuk bağlamında ele alınmasıyla betimleyici, ilişki arayıcı ve sorun çözücü bir yöntem benimsenmiştir.

Bu çalışmamız bilişim hukuku, uluslararası hukuk, kamu yönetimi, güvenlik bilimi ve yönetim bilişim sistemleri disiplinlerinin kesişiminde çok disiplinli bir yaklaşım ortaya koymaktadır. Ortaya atılan savımız da bu disiplinlerin ortak inceleme nesnesi içerisinde kabul edilebilir. "bilişim yönetişimi" öz itibariyle bu farklı disiplinlerin bir birisiyle ahenk içerisinde kullanılmasını gerektirmektedir.

Şekil 9.1. Farklı Bilim Dallarının Kesişiminde Siber Yönetişim
(**Kaynak:** Araştırmacılar tarafından hazırlanmıştır.**)**

Siber yönetişim paradigması aşağıdaki soruların cevaplanabilmesine dayanmaktadır:

1. *Siber alanı kimler yönetmelidir?*
2. *Siber alan yasal (formel) ve yasadışı (informel) alanda nasıl yönetilmelidir?*

Bu çalışmamızda yukarıdaki sorulara bilişim hukuku ve uluslararası hukuk kapsamında analizler ve bir BT yönetişim çerçevesi olan COBIT-5 ile değerlendirmeler yapılarak 2016-2019 Ulusal Siber Güvenlik Stratejisinin bu sorulara cevap verebilme yetkinliği araştırılmakta ve bu çerçevede elde edilen sonuçlar ışığında bir siber yönetişim modeli oluşturulmaya çalışılmaktadır. Bu kapsamdaki analizlerimizde öncelikle uluslararası hukukun bilişim hukukuyla kesişiminde siber teröre karşı siber güvenlik ele alınacak, bilişim hukuku ve ceza hukuku kapsamında değerlendirmeler yapılacak, ihlallerde devletin sorumlulukları, AB siber güvenlik stratejisi ile Türkiye siber güvenlik stratejileri incelenerek COBIT-5 bilişim yönetişimi modeli kapsamında analiz yapılacak, yönetimin yönetişim ile ayrışmasına değinildikten sonra siber yönetişim modelinin bileşenleri ve gereklilikleri tespit edilerek bir model önerisi yapılacaktır.

9.3. Küresel Siber Teröre Karşı "Siber Güvenlik Yönetişimi"

Son zamanlarda teknolojinin gelişmesine paralel olarak elektronik olanakların ve cihazların daha ucuz ve verimli olması sanal alanı genişletmiş ve bulut bilişim üzerinden yapılan işlemlerin nicelik ve niteliğini arttırmıştır. Bu durum tabii olarak siber alandaki risklerin özellikle bulut bilişim üzerinden ciddileşmesine yol açmıştır. Özellikle bulut bilişim kullanıcılarının karşılaşabilecekleri sorunlar iç, dış ve veri koruma riskleri olarak üç başlıkta incelenmiştir. Bunlar; İç güvenlik riskleri kapsamında; eski çalışanların şifrelerinin iptal edilmemesi, kullanıcıların kendi kullanıcı adı ve şifrelerini güvensiz ortamlarda kullanmaları, zayıf kullanıcı ismi ve şifreleri şeklinde sıralanmıştır. Dış güvenlik riskleri kapsamında; servis sağlayıcısı teknolojik hatası yüzünden oluşan güvenlik sorunları, servis sağlayıcısı çalışanlarının dikkatsizliğinden doğacak bilgisayar korsanlığı olarak sıralanmıştır. Veri koruma riskleri kapsamında ise; verilerin nerede tutulduğu veya nerelere dağıldığı, kimlerin veriye erişebil-

diği gibi riskler belirtilmektedir. Kullanıcıların karşılaşabilecekleri bir diğer sorun, siber saldırılara maruz kalabilen bulut bilişim kaynaklı kesintileridir. Bu kesintiler buluta bağlı çalışan şirketlerde iş kaybına ve böylelikle maliyet artışına sebep olacaktır. Örneğin, Salesforce'un 2009 yılında yaşadığı 38 dakikalık kesinti nedeniyle milyonlarca müşteri, verileri kitlendiği için işlem yapamamışlardır. 2010 yılında ise iki gün boyunca 300.000'den fazla müşteri Intuit'in çevrimiçi hizmetlerine ulaşamamıştır [29]. Bulut alanda saklanan verilerin artması ve kritik hizmetlerin bulut üzerinden yürütülmesi siber saldırıların bu alanlara potansiyel olarak yoğunlaşabilmesi ve siber savaşların meydana gelmesine yol açmaktadır.

Ordunun da siber güvenlik stratejilerine katılması ve roller üstlenmesi için gerekli ve yeterli risk ve tehditler mevcuttur:

- Hükümetten ve savunma müteahhitlerinden bilgi çalınması, muhtemelen ulusal güvenlik için en ciddi tehditler arasında yer almaktadır. Ticari izin de dahil olmak üzere bu tür izinsiz girişler için çeşitli olası motivasyonlar vardır, ancak bunlar gelecekteki askeri etkililiğin bir tavizini de temsil eder.
- Ulusal altyapıda kritik öneme sahip yıkıcı bir saldırı potansiyeli (finans, enerji, ulaşım, iletişim ve bir milletin yaşamı için hayati öneme sahip diğer ekonomik sektörler de dahil olmak üzere), ulusal güvenlik sırlarının çalınmasından daha az acil olsa da, ciddi bir endişe kaynağıdır.
- Ticari casusluk, fikri mülkiyete ait veya hassas ticari bilgilerden oluşmakta ve askeri yaklaşımların uygun olamayabileceği bir başka alan olarak kategorize edilmektedir. Bununla birlikte, potansiyel ekonomik etki göz önüne alındığında, özellikle devlet destekli Gelişmiş Kalıcı Tehdit (APT) teknikleri kullanıldığında, bu tür bir faaliyet uluslararası ilişkileri önemli ölçüde belirleme potansiyeline sahiptir.
- Dördüncüsü, siber suç tehdidi var. Doğrudan bir tehdit olmasa da, teröristlerin ya da devletlerin suç ağlarından yararlanma potansiyeli nedeniyle kontrol edilmezse ciddi bir hal alabilir.

Ancak şunu da unutmamak gerekir ki tam otomasyon, internet ve iletişim teknolojilerinden faydalanılarak işlenen bilişim suçları ile mücadele etmek oldukça zor ve pahalı bir iştir. Yeterli teknik bilgiye

sahip personel ve bu personelin ihtiyacı olan teknik altyapıya sahip olmak bu suçlarla mücadele edebilmenin olmazsa olmaz koşuludur. Bilişim suçlarıyla mücadelede karşılaşılan temel sorunlar; suçu işleyen kişinin, suçun işlendiği yerin, suç işlenen cihaz ya da sistemin ve suçun ne zaman ve nasıl işlendiğinin tespitinin zor olduğu şeklinde sıralanabilir. Ayrıca bilişim suçlarıyla mücadelenin temel dayanağı ve olmazsa olmazı olan yeterli mevzuat da (kanun, tüzük, ve yönetmelik gibi) göz ardı edilmemelidir. İnternetin olduğu her yerde muhakkak hukuk kuralları etkin şekilde işle(til)meli ve siber suçlar cezalandırılmalıdır.

Ülkeler arasında işbirliği yapılmalı ve siber suçlara karşı iletişim içinde olunmalıdır. Her ülkede siber suçların cezası çok ağır olmalı ve eğer yoksa ülkeler arasında siber suçlar ile ilgili hukuki bağlar ivedilikle kurulmalıdır. Yani internet nasıl ki uluslararası bir niteliğe sahipse bu suçlar ile mücadelede uygulanacak hukuk kuralları da evrensel olmalı ve herkesin üzerinde mutabık olduğu küresel yasal bir sistem olmalıdır. Eğer bilişim devriminin de bir sınırı olması gerekiyorsa bu sınır her ülkede uygulanacak olan evrensel normlar olmalıdır. Her ülke kişisel verilerin korunmasına dair düzenlemeler yapmalı ve iç hukuklarını da buna göre ayarlamalıdırlar [52].

Siber Yönetişimin kapsadığı alanlar aşağıdaki hususlardır [27]:

- Siber uzayda kayda değer bir güvensizlik: giriş engelleri düşüktür ve suç ve savunma maliyetleri arasında bir asimetri vardır;
- Hükümetler BM-ITU çerçevesinde ulusal spektrum tahsisini yönetmektedir;
- BM tüzüğünde, Silahlı Çatışma Yasaları (LOAC), güvenlik ve casusluk sorunlarını yönetmek için bir çerçeve sunar;
- Pratikte birçok özel ve kamu yönetişimi alanı vardır;
- Güvenliği sağlamak, devletin temel bir işlevidir;
- Şiddetli siber casusluk faaliyetleri giderek yaygınlaşmaktadır;
- Hükümetler, toplumlarının yararı için interneti korumak istemektedirler, fakat aynı zamanda toplumları internetten gelecek olanlardan korumak istemektedirler: sansür uygulaması (örneğin: google, twitter, FB, vb.)

Siber yönetişim, teknolojinin yeni oluşumu ve volatilitesi nedeniyle zordur. Siber konuları karşılaştırmak için boyutlar derinlik, genişlik, doku ve uyumluluktur:

1. *Derinlik,* bir dizi kuralın veya normun hiyerarşik tutarlılığını ifade eder (ör., Alan adları).
2. *Genişlik*, bir dizi normu kabul eden devlet ve devlet dışı aktörlerin sayısının kapsamını ifade etmektedir (ör. Budapeşte Sözleşmesi, 42 devlet).
3. *Doku*, bir sorun alanındaki devlet ve devlet dışı aktörlerin karışımını ifade eder (ör. Savaş yasaları).
4. *Uygunluk*, bir dizi normlara (ör., Alan adları ve protokoller) davranışsal bağlılığın ne kadar yaygın olduğunu ifade eder.

9.4. Siber Yönetişimde Devletin, Kurumların ve Kişilerin Sorumluluğu

Askeri veya istihbarat birimler tarafından ya da her hangi bir kamu tüzel kişiliğini haiz kurum veya kuruluş tarafından yapılan ihlaller devletlerin sorumluluğundan birinci önceliği taşımaktadır. Buna kısaca "*devletin siber eylemleri*" olarak tanımlama yapılabilir. Devlete bağlı olmayan varlıklar tarafından işlenen ihlaller yani, devlet tarafından teşvik veya kontrol edilen geçici gruplar, devlet tarafından kontrol edilmeyen ulusalcı veya vatansever hacker grupları ile terörist hacker grupları tarafından işlenen ihlaller de "*devlet dışı siber eylemler*" olarak tanımlanmaktadır [47].

Bir siber operasyon pek çok uluslararası yükümlülüğü ihlal edebilir. NATO tarafından yayımlanan TALLINN Rehberine göre[1], bir siber operasyonun güç kullanımı kapsamında değerlendirilmesinin tespit edilebilmesini sekiz ölçüte bağlamıştır. Bunlar; *şiddet* (kaç insanın öldürüldüğü, ne kadar geniş alanda saldırı yapıldığı, ne kadar zarar verildiği), *anilik* (siber eylemin etkilerinin ne kadar yakında hissedilmeye başlanacağı, bu etkilerin oluşumunu destekleyen ey-

1 Tallinn Rehberi, e-demokrasi ve e-devlet Dünya klasmanlarında birinci olan ve her türlü kamu hizmetini elektronik uygulamalarla entegre hale getirmiş olan Estonya'nın siber saldırılar ile haftalarca sistemlerinin işlemez hale gelmesi üzerine Estonya Tallinn şehrinde uzun süren çalıştaylar ve araştırmalar sonucunda NATO'nun sahiplendiği bir siber güvenlik rehberidir. Detaylı bilgi için bkz: https://ccdcoe.org/research.html

lemlerin devam edip etmediği), *doğrudanlık* (yapılan eylemle sonuçlar arasında illiyet olup olmadığı, bunların meydana gelecek etkileri arttırmada bir etken olup olmadığı), *kuşatıcılık* (eylemde güvenliği sağlanan bir elektronik ağı ele geçirmeye çalışılıp çalışılmadığı, eylemlerin mihrak noktasının hedeflenen ülke olup olmadığı), *ölçülebilirlik* (eylemin etkilerinin nasıl sayısallaştırılabileceği, eylem sonuçlarının paralel veya farklı rakip saldırılarla karıştırılıp karıştırılmadığı), *askeri nitelik* (askeri birimlerin siber operasyona dâhil olup olmadığı, siber operasyonlarda askeri birimlerin hedeflenip hedeflenmediği), *devletin müdahil olması* (devlet veya kamu birimlerinin doğrudan veya dolaylı bir şekilde operasyona dâhil olup olmadığı, devletin dahil olmaması durumunda eylemlerin gerçekleşebilir olup olmadığı) ve *varsayımsal yasallık* (eylemin kategorik olarak güç kullanımı olarak karakterize edilip edilmeyeceği, kullanılan araç ve tekniklerin uluslararası hukuk kapsamında meşru olarak nitelendirilebilen bir nitelikte olup olmadığı) gibi kriterlerdir.

Bu kriterler uluslararası hukukun hangi ölçüde ihlal edildiğini tespit ve değerlendirmede kullanılmaktadırlar. Aşağıda güç kullanımı, güç tehdidi gösterimi ve adem-i müdahale gibi yasaklar siber operasyonlar kapsamında değerlendirilmektedir.

Bu yukarıdaki kriterler kapsamında bir siber eylemin güç kullanımını içermediği ve fiziksel, kişisel veya mülkiyet anlamında bir zarara yol açmadığı tespit edildiğinde TALLINN Rehberi burada siber eylemlerle geleneksel eylemler arasındaki nüans farklarının belirlenmesini gerekli kılmaktadır. Güç kullanımının dar anlamdaki tanımına göre, sadece askeri gücü içermesi (politik ve ekonomik zoru dışlayıcı bir şekilde) fiziksel zararlara yol açmayan siber saldırıların güç kullanımı kategorisinde sayılmaması gerekir. Zarar vermeyen bir siber saldırının geleneksel güç kullanımı altında zikredilmesini gerektirir ki bu da güç kullanımı yasağı kapsamının dışına çıkması anlamına gelmektedir. Örneğin TALLINN'e göre bir hükümette veya ekonomide güven bunalımına yol açacak şekilde yapılan siber psikolojik eylemlerin güç kullanımı olarak tanımlanmaması gerekmektedir. Örneğin bir zararlı yazılımla hava savunma sisteminin uzun bir düze etkisizleştirilmesi güç kullanımı olarak kabul edilir. Dolayısıyla geleneksel anlamda askeri güçlerle bir ülkeyi kuşatmadan beklenen sonuçlar gibi fiziksel zararların meydana gelmesi ge-

rekir ki bir siber eylem güç kullanımı olarak nitelendirilebilsin. Aksi durumlarda bu kategoride kabul edilmemektedir [22, 23, 34].

Bir siber operasyon aynı zamanda güç gösterimi yasağının da ihlal edilmesine yol açabilir. Bu yasak Birleşmiş Milletler Tüzüğünde mevut olmakla birlikte uluslararası hukukta iyice belirlenmiş olmadığından geleneksel anlamda uygulanmaktadır. Yasal veya meşru bir gerekçesi olmadan güç kullanımı noktasında istekliliğin ifade edilmesi yasak bir güç gösterimi olarak kabul edilir. Buradaki tehdit, güç kullanılmasının ifade edilmesidir. Bir ülkenin hava savunma sisteminin başka bir ülke tarafından etkisiz hale getirilmesi füze, bomba veya hava operasyonu yapılacağına dair güç kullanımı ifadesi kapsamında bir tehdit olarak kabul edilebilir. Hava savunma radar veya füze karşılama sistemlerinin devre dışı bırakılması kapasitesinin aşırı bir şekilde gösterilmesi bir devletin meşru gerekçe olmaksızın konvansiyonel silahlarla saldırı yapması noktasında istekliliğini ifade edebilir. Siber operasyon ile bu şekilde bir teşebbüs bile başlı başına bir devletin başkasına karşı güç kullanmada karşılık ve savunma istemediğinin ifadesi olabilir. Siber saldırılar için bu şekilde bir potansiyel olmakla birlikte çoğu siber saldırıda daha çok devletin belirli organlarının web sayfalarına saldırılması veya jeopolitik ya da ekonomik değere sahip hassas bilgilerin ele geçirilmesini hedeflemektedir [46].

Bir siber operasyon aynı zamanda adem-i müdahale[2] ilkesini de ihlal edebilir. Bu ilke, toprak hükümranlığından kaynaklanmakta ve geleneksel uluslararası hukuk içerisine gömülüdür. Bu ilke, her bağımsız ülkenin kendi işlerini başkalarının müdahalesi olmaksızın icra etme hakkını korumaktadır [47]. Ulusal istiklali göstermektedir. Bu durumda siber operasyonlar kapsamında toprak hükümranlığı veya ulusal istiklal nasıl zarar görebileceği tartışma konusudur. Bu analiz kabul edilebilir dış politika (başka ülkelere ekonomik yaptırımlar, olaylar üzerinde politik yorumlar) ile kabul edilemez müdahaleler (bir ülkenin müdahale edilen bir konuda kontrol iktidarından mahrum bırakılması) arasında ayırım yapılması gerekir. Bir network saldırısında vatandaşlara ait kişisel, mali veya mülkiyete ait bilgilerinin değiştirilmesi veya bozulması durumunda devletin kendi sorumluluk alanında gerekli kontrol ve iktidardan mahrum

2 Principle of non-intervention

olmasına yol açılmış olabilir. Saldırıda hedeflenen ülke network sızmasını vatandaşlarının mahremiyetinin ve mülkiyet hakkının ihlal edilmesi olarak görerek kendi iç işlerine karışılması şeklinde kabul edebilir. Sony olayında olduğu gibi Kuzey Kore Devleti, bir filmin ABD piyasasında satılması engellenmiştir. Bu durumda vatandaşlık hakları veya devletin bağımsızlık ve istiklali zarar görmemiş olmakla birlikte politik, ekonomik veya sosyal yönlerden devletin çıkarları zedelenmiştir [47].

Dolayısıyla NATO tarafından hazırlanan TALLINN Rehberi aslında siber alandaki hak ihlallerini önlemek ve ulusal devletler arasında belirli bir norm birliği oluşturmaya ve bu alanda bir altyapı tesis edilmesini hedefleyen bir çalışma olarak göze çarpmaktadır. Bu çalışma zamanla yerel ve ulusal otoriteler ile mahkemeler tarafından referans alınarak yasal düzenlemelerle yargısal içtihatların belirli bir yönde oluşmasına katkıda bulunacağı söylenebilir. Bu çalışma aslında oluşturduğu farkındalık ile siber yönetişim için de bir zemin tesis etmektedir [50, 61].

Kişisel verilerin korunması kapsamında kamu kurum ve kuruluşlarına da sorumluluk getirilmiştir. Özellikle kişisel verileri saklayan ve yöneten kurum ve kuruluşlardaki yöneticiler bireysel olarak da ihmal ve suiistimallerden sorumlu tutulabileceklerdir. TCK'nın 136. maddesine göre: "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır". TCK'nın 135. maddesindeki düzenlemeye benzer şekilde kişisel verilerin üçüncü bir kişiye verilmesi, yayılması ya da ele geçirilmesi suçlarının hukuka aykırılık ön koşuluna bağlandığı görülmektedir. TCK'nın nitelikli hallerin düzenlendiği 137. maddesine göre: "Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır."

TCK'nın 138. maddesine göre:

"(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

(2) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır".

TCK'nın 138. maddesinde şikâyet usulü düzenlenmektedir. Buna göre, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikâyete bağlıdır.

TCK'nın 138. maddesinde, yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı belirtilmektedir. Bu kapsamda devlet otoriteleri ve kamu görevlileri de sorumlu olabilir.

Kişisel Verileri Koruma Kanununun 18. maddesi şöyledir [45]:

" (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,

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".

Kanunun 18. maddesinde yer alan, idari para cezası miktar aralığı oldukça geniştir. Gerekçede, Kurulun idari para cezasının miktarını belirlerken 5356 sayılı Kabahatler Kanunu'nun 17. maddesi uyarınca kabahati işleyenin ekonomik durumunu, kabahatin haksızlık içeriğini ve failin kusur derecesini dikkate alacağı belirtilmiştir. İdari para cezaları, veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanacaktır. Maddede kabahat olarak düzenlenen eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde, 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 yapılacaktır. İlgili kurumlar yaptıkları soruşturmanın sonuçları hakkında Kurula bilgilendirme yapmak zorundadır.

9.5. Ulusal Siber Güvenlik Stratejisi ve Eylem Planında Yönetişim

2013-2014 döneminde gerçekleştirilmesi planlanan işlere ilave olarak bu yılları aşan periyodik faaliyetler ile eğitim ve bilinçlendirme çalışmaları gibi sürekli yürütülmesi gereken faaliyetlere yer veren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 20/06/2013 tarih, 28683 sayılı Resmi Gazete'de yayınlanarak yürürlüğe girmiştir. Gelişen bilgi ve iletişim teknolojileri, artan güvenlik gereksinimi ve edinilen tecrübeler doğrultusunda, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından ulusal siber güvenlik stratejisinin güncellenmesi ve 2016-2019 dönemini kapsayan eylemlerin belirlenmesi ihtiyacı doğmuş ve "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" hazırlanmıştır. Aşağıda her iki strateji kısaca incelenmektedir.

Önceki dönem strateji ve eylem planı süresinin dolması nedeniyle yeni bir strateji ve eylem planı hazırlanmıştır. Ancak önceki eylem planının ne kadarının gerçekleştirilip ne kadarının gerçekleştirilmediği konusu hakkında kamuoyuyla paylaşılan bir araştırma raporu veya analiz mevcut değildir. Yeni dönem eylem planının bir farkı da öncekinin açık ve erişilebilir olmasına rağmen yenisinin kamuoyuyla paylaşılmayan ve ancak hizmete özel ilgili kurumların bilgisinde gizli tutulmuş olmasıdır [43].

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının ana amacı; siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılması olarak belirlenmiştir. Bu ana amacı gerçekleştirmek üzere, hedeflerin ve alt eylem maddelerinin belirlenmesi, bunların gerçekleştirilmesinin sağlanması ve denetlenmesi de bu dokümanın amaçlarındandır. Bu amaçlar doğrultusunda:

- Ulusal siber uzayın tamamını kapsamak şartıyla, bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve bilgi/veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin, gizliliğinin ve mahremiyetinin sağlanmasına,
- Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kolluk kuvvetlerince daha etkin araştırılmasının ve soruşturulmasının sağlanmasına,
- Siber güvenliğin, gizliliğin ve mahremiyetin sağlanmasında kritik teknolojilerin ve ürünlerin ülkemizde üretilmesine, üretilemiyorsa, dışarıdan alınan teknoloji ve ürünlerin salt bu maksatla ve güvenle kullanılabilmesini sağlayacak önlemlerin alınmasına yönelik bileşenler bu planda yer almaktadır [7, 8].

Önceki plandan farklı olarak yeni planda siber güvenliğin ilkeleri de riskler ve eylemlerle birlikte belirlenmiştir.

9.5.1. Siber Güvenlik İlkeleri

2016-2019 Siber Güvenlik Stratejisi ve Eylem Planında ise aşağıdaki ilkeler yer almaktadır [7, 8]:

1. Siber güvenlik, risk yönetimini esas alan etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı yöntemler aracılığıyla sağlanır. Oluşturulan risk yönetimi metotlarının tehdit ve açıklıkları ele alarak bunlardan dolayı ortaya çıkacak riskleri belirlemesi, bu riskleri kabul edilebilir düzeye indirmek için yöntemler sunması hedeflenir.

2. Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir. Bu farkındalık ve yetkinliğin sağlanması için tüm paydaşların gerekli eğitim ve deneyimi kazanmaları sağlanır. Teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutları da içeren bütüncül bir yaklaşım benimsenir.
3. Risk yönetimi, teknik zaafların hızla giderilmesini, saldırı ve tehditlerin önlenmesini, fark edilmesini, yanıtlanmasını ve muhtemel zararın en aza indirgenmesini içerir. Zararların asgari düzeyde tutulması için siber olaylara karşı bir hazırlık ve süreklilik planının bulunmasına ve uygulanmasına önem verilir.
4. Siber uzay güvenliğinin sağlanması ve sürdürülmesinde; kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir ve güven inşa edilir.
5. Tüm paydaşlar, siber uzay güvenliğinin sağlanması için çalışırken, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkelerini gözetir.
6. Paydaşlar siber uzaydaki risklerin yönetimi ile ilgili sorumluluklarını yerine getirirken şeffaflık, hesap verilebilirlik ve etik değerleri göz önünde bulundurur.
7. Alınan siber güvenlik önlemlerinin ilgili risklerle orantılı olması, olumlu ve olumsuz etkilerinin değerlendirilmesi ve dengelenmesi sağlanır.
8. Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, yenilikçilik anlayışı esas kabul edilir.

9.5.2. Siber Güvenlik Riskleri

Siber güvenlik kapsamında stratejik amaçların en doğru şekilde tanımlanabilmesi için siber güvenlik riskleri gerçekçi bir biçimde değerlendirilmiş ve belirlenen başlıca riskler aşağıda sıralanmıştır [7, 8]:

1. Kritik altyapıların kullandığı bilişim sistemlerine yapılacak hizmet dışı bırakma ve benzeri hedef odaklı saldırılar sonucunda enerji, ulaştırma, vb. kritik hizmetlerin kesintiye uğraması.
2. Kamu ve kritik altyapıların kullandığı bilişim sistemlerine yapılacak hedefe yönelik saldırılar sonucunda; vatandaşa ait kişisel bilgilerin veya kamuya ait gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
3. Araştırma, geliştirme ve üretim yapan kurum ve kuruluşların (özel firmalar, araştırma kurumları ve savunma sanayi) ticari sırlarını ve bilgi birikimini elde etmeye yönelik hedef odaklı saldırılar sonucunda hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
4. Propaganda amaçlı bilgisayar korsanlığı (hacktivizm) saldırıları sonucu çeşitli kurum ve kuruluşların itibarının zarar görmesi veya hassas bilgi/verinin ifşa olması, değiştirilmesi veya yok edilmesi.

5. E-ticaret yapan kuruluşların, E-posta hizmeti veren kuruluşların, sosyal medya hizmeti veren kuruluşların hizmet dışı bırakma ve benzeri saldırılar sonucunda hizmet verememesi nedeniyle maddi kayba uğraması, sahte işlem kaydı oluşturulması, gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
6. E-ticaret yapan kuruluşların, finans sektörü veya çevrimiçi ödeme ya da para transferine imkan veren diğer kuruluşların müşterilerine ait hassas bilgilerin saldırganlar tarafından ele geçirilmesi nedeni ile itibar kaybına uğraması, toplumda çevrimiçi işlemlere yönelik güven kaybı oluşması, bu hizmetlerden faydalanan müşterilerin maddi kayba uğraması.
7. Küçük ve orta ölçekli sanayi, ticaret ve hizmet sektöründeki kuruluşların faaliyetlerinin bilişim sistemlerindeki güvenlik önlemlerinin eksikliğinden veya kullanıcı hatalarından dolayı kesintiye uğraması, hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

8. Toplumun internete ve sosyal ağlara olan bağımlılığı, siber güvenlik alanında yeterli düzeyde bilgi ve bilinç seviyesine sahip olmaması, mobil ve sabit bilgi sistemlerinde kişisel güvenlik önlemlerini almaması gibi nedenlerle kötücül yazılım ve oltalama saldırılarına, dolandırıcılık ve kimlik hırsızlığına maruz kalması, kişisel bilgilerin ve cihazların saldırganlar tarafından ele geçirilmesi, değiştirilmesi veya yok edilmesi, sahte işlem yapılması.
9. Her türlü kurum ve kuruluşta yığın posta, kötücül yazılım ve benzeri saldırılar sonucunda dolandırıcılıkla karşı karşıya kalınması.
10. Her türlü kurum ve kuruluşta, kullanıcı hataları ya da doğal afetler sonucunda bilişim sistemleri aracılığı ile verilen hizmet ve faaliyetlerin kesintiye uğraması.

9.5.3. Stratejik Siber Güvenlik Amaçları ve Eylemleri

2016-2019 döneminde, mevcut riskleri, belirlenen ilkeler ışığında asgari düzeye indirmeyi hedefleyen stratejik amaçlar şunlardır [7, 8]:

1. Ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar) tarafından denetlenmesi.
2. Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması.
3. Sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi.
4. Kurumların bilişim sistemlerinin sadece saldırılardan değil, kullanıcı hataları ve afetlerden de korunması için düzenlemelerin yapılması.
5. Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması.
6. Siber güvenlik konusunda kurum yöneticilerinin farkındalığının artırılması.
7. Siber güvenlik alanında yetkin personel yetiştirilmesi ve bu alanda uzmanlaşmak isteyen personel, araştırmacı ve öğrencilerin teşvik edilmesi.

8. Toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması.
9. Kamu kurumlarında siber güvenlik alanında uzman personel istihdam edilmesi için mevzuat desteği sağlanması ve personelin özlük haklarının iyileştirilmesi.
10. Kurumsal ve Sektörel SOME'lerin (Siber Olaylara Müdahale Ekibi) etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, yetkin personel ihtiyacının karşılanması, bilişim altyapısının sağlanması ve ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımının geliştirilmesi.
11. Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması.
12. Kamu kurumları, özel sektör, STK'lar (Sivil Toplum Kuruluşu), denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyon hedefi ile ulusal siber güvenlik eko-sisteminin oluşturulması.
13. Ulusal Siber güvenlik eko-sistemi içinde iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması.
14. Bilişim sistemlerinin kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin içerdiği açıklıkların kötüye kullanılmasına engel olmak üzere açıklık analizi ve sertifikasyon çalışmalarının yapılması.
15. Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması.
16. Siber güvenlikte dışa bağımlılığı azaltmak için Ar-Ge faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi.
17. Tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi.
18. Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliği ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılması.

9.6. Ulusal Siber Güvenlik Stratejisi ve Eylem Planının BT Yönetişimi Değerlendirmesi

Bu çalışmamızda 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın bilişim hukuku ile uluslararası hukuk kapsamında analiz edilerek bütünlükçü bir yaklaşımı ortaya koyma noktasındaki eksikliklerinin ortaya konularak bunların nasıl giderilebileceğine dair bir yaklaşım sergilenmiştir. Bu maksatla da COBIT-5 çerçevesinin temel özelliklerine değinmekte yarar görülmüştür.

Bir paradigma olarak dikkate alınabilecek olan COBIT, önceleri denetim, kontrol ve daha sonra yönetim çerçevesi iken daha sonraları risk ve katma değer ile ilgili standartları da bünyesine alarak zamanla bir BT yönetişim çerçevesi haline gelmiştir. Her versiyonunda paradigmatik bir kırılımla kendisini yenileyen COBIT-5 versiyonunda, en sonunda sadece BT değil diğer iş süreçlerini de kapsayarak kapsamlı bir model haline gelen bütünlükçü, kapsayıcı ve uyarlayıcı bir çerçeve iddiasındadır. COBIT-5 ile ortaya konulan ilkeler ve gerçekleştiriciler ile BT yönetişiminin iş süreçleri ile birlikte yönetilebilmesine olanak sağlayacak bir yönetişim ve yönetim modellemesi süreçleriyle birlikte ortaya konulmaktadır [26, 54].

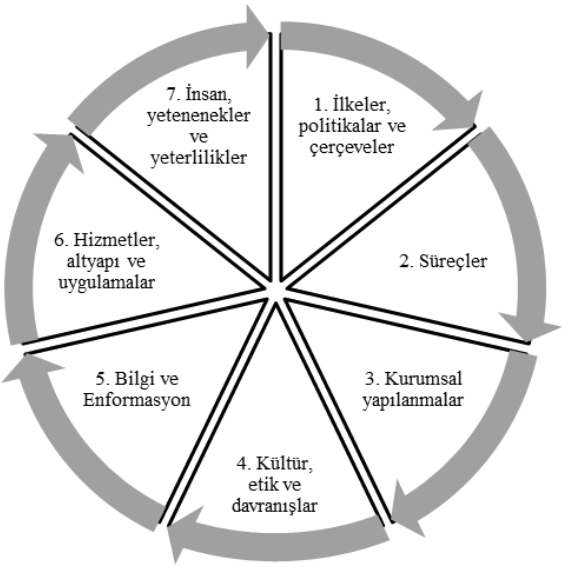
COBIT, ilk başta finansal ve BT denetim ve kontrol alanlarında ilk önce kendisini göstermişti. İlk baştaki COBIT, "*Control Objectives of IT*" olarak bilinmekteydi. Daha sonra COBIT, göstergeler, süreç araçları, kritik başarı faktörleri, olgunluk modelleri ve BT yönetimi ile ilgili görev ve sorumluluklarının yerine getirilebilmesi için geliştirilen araçlarla birlikte aşamalı bir şekilde toplumsal ve ekonomik koşulların sonucu olarak yeni olarak elde edilen bilgilerle girdiği paradigma gerilimleri sonucunda bir yönetişim ve yönetim çerçevesi haline gelivermiştir. Paradigma gerilimi, diğer standart ve çerçevelerin mevcut teknik ilişkiler ağını, gereklilikleri ve sürdürülebilir stratejik yönetimi acımasız rekabet ortamında açıklayamaması ve çözüm bulamamasından dolayı ortaya çıkmıştır. Çünkü her kurumun paydaşları ve ihtiyaçları farklı olduğundan ve kaynakları ile riskleri de aynı olmadığından kendilerine has uyarlamaların yapılabilmesi aşikâr bir halde belirginleşmiştir. Kendisini çevresel koşullara ve zamanın gereklerine göre sürekli adapte edebilen COBIT bu gerilim içerisinde yeni bir paradigma olarak ortaya çıkarak mevut sorunlara çözüm sunma iddiasındadır.

COBIT-5 çerçeve yaklaşımı 5 temel ilke *"principles"* getirmektedir. Bu ilkeler çerçevenin esas sütunlarını teşkil etmektedirler. Bu ilkeler üzerinde yapılacak olan yapısal kurgu ve süreç uygulamaları da gerçekleştiriciler *"enablers"* vasıtasıyla temellendirilebileceklerdir. Bu ilkelere göre bir kurumda öncelikle yapılması gereken iç ve dış paydaşların ihtiyaçlarına odaklanan bir yaklaşım ortaya konulması gerekliliğidir. Daha sonra kurumun tüm yapılarını kapsayan tüm kaynaklarını kullanan tek bir çerçeve modelin uygulanarak iş ve bilişim süreçlerine bütüncül yaklaşım sergilenmesi gerekmektedir. En nihayetin de karar alma mekanizması olan yönetişim ile uygulama mekanizması olan yönetimin süreçler bazında ayrıştırılması gerekmektedir. Bu ayrışmada 5 adet ana yönetişim süreci tesis edilirken 32 adet yönetim süreci tesis edilmekte ve bu tüm süreçler birbirilerine girdi alıp vermektedir. En önemlisi de kurumun amaçları, paydaşların ihtiyaçları ve BT ile ilgili hedeflerin yönetim ve yönetişim süreçlerinde ölçülebilir göstergelerle takip edilmesine ve süreçlerin olgunlaştırılmasına olanak sağlayan teknik bir analiz ve uygulamanın kurgulanmasıdır [26, 54].

Şekil 9.2. COBIT-5 Temel İlkeleri [26]

Şekil 9.2'de görüldüğü gibi COBIT-5 beşinci versiyonunda beş temel ilke üzerinde kurulmuştur. COBIT-5, sistem teorisinin temel varsayımlarını kullanarak birbiriyle etkileşim içerisindeki bileşke-

leri dikkate alarak bütüncül bir yaklaşım sergilenmesi gerektiğini ortaya koymaktadır. Buna göre, Şekil 9.3'de verilen gerçekleştiriciler kurumsal yönetişim ve yönetim açısından birbirini bütünleyen, diğer çerçeve ve standartların eksikliklerini tamamlayan, kurumun varlığını sürdürmesi için gerekli olan alt sistemlerden oluşan canlı bir sistemin birliğini tamamlamaktadır [26].

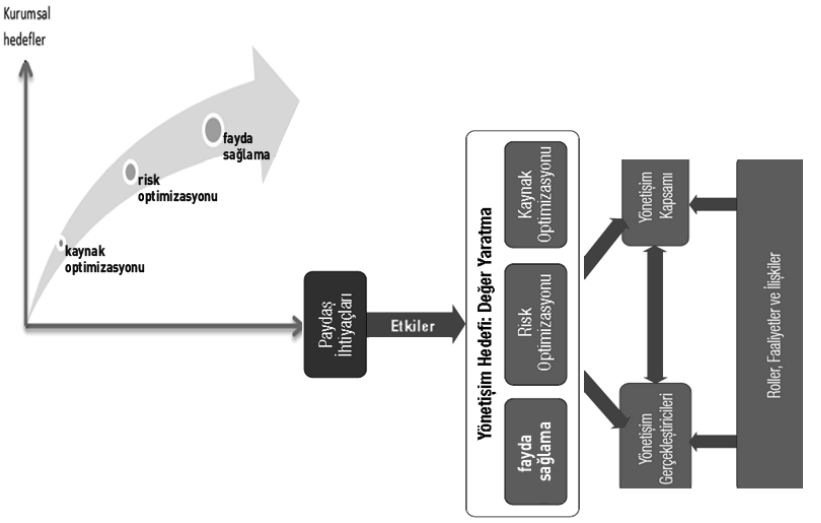


Şekil 9.3. COBIT-5 Gerçekleştiricileri [26].

COBIT-5 gerçekleştiricileri bütüncül yaklaşımı esas alınarak BT ve iş süreçleri ile birlikte bir kurumsal anlamdaki her şey gerçekleştiriciler kapsamına alınabilmektedir. COBIT-5 ile gelinen noktada yönetişimin paydaş ihtiyaçlarının belirleme, kurumsal amaçlara dönüştürme ve bununla ilgili BT hedeflerini belirleme alanında yönlendirme, değerlendirme ve izleme olarak 3 ana süreçte belirlenmiş olup, bunların diğer yönetim süreçlerinden ayrıştırılması esası benimsenmiştir.

Buna göre, kurumsal yönetişim karar alma mekanizması ile kendi içerisinde bulunduğu özgün çevre ve ekosistemin içsellik ve dışsallıklarına göre değişebilen paydaş ihtiyaçlarına göre hedeflerin tekrar gözden geçirilerek mevcut kaynakların optimal kullanımı, risklerin en iyi yönetimi yoluyla katma değer oluşturacak şekilde kurumsal hedeflere ve BT ilişkili hedeflere dönüştürülerek yönetime yön verme mekanizması olarak anlaşılmaktadır. Paydaş ihtiyaç-

ları ile kurumsal hedeflenmelerin tutarlılığı nispetinde kaynak ve risk optimizasyonu yapılarak katma değer elde edilebilir.



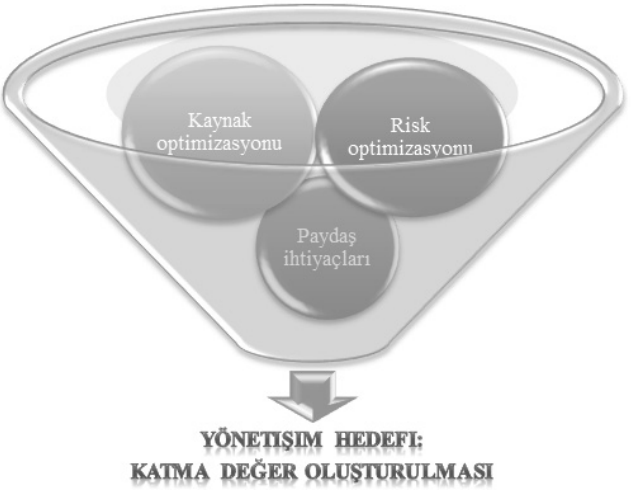
Şekil 9.4. Paydaş ihtiyaçlarına göre kurumsal hedeflemenin yapılması gerektiğini gösteren şekil
(Kaynak: Araştırmacılar tarafından oluşturulmuştur.)

Buradaki risk optimizasyonu, kurumsal amaçları olumsuz etkileyen etkenleri mevcut kaynaklar ve elde edilecek faydanın dikkate alınmasıyla uygulanacak tedbir ve önlemlerin en iyileştirilmesidir. Bunun sağlanması için de roller, faaliyetler ve ilişkilerin yönetişim kapsam ve gerçekleştiricileri dikkate alınarak belirlenmesi gerekir.

Şekil 9.5'de görüleceği üzere, COBIT-5 yönetişim hedefi, katma değer oluşturmaktır. Bu katma değer de ancak paydaş ihtiyaçlarının yerine getirilmesi amacıyla kaynakların ve risklerin optimize edilmesiyle elde edilebilir.

Yönetişim paradigması ile başlayan yönetişim ekolü veya yönetişimci akım, bilgi yönetimi ve Yönetim Bilişim Sistemleri (YBS) alanına da sızarak Bilişim Teknolojileri Yönetişimi (*IT Governance*) ifadesi ile kendisini tanımlamıştır. Aşağıda daha detaylı bir şekilde ortaya konulacağı üzere, BT Yönetişim Enstitüsü[3] tarafından icat edilen bu yepyeni paradigma pek çok kavramı bünyesine almaya meyilli görülmektedir.

3 Detaylı bilgi için bkz: http://www.itgi.org

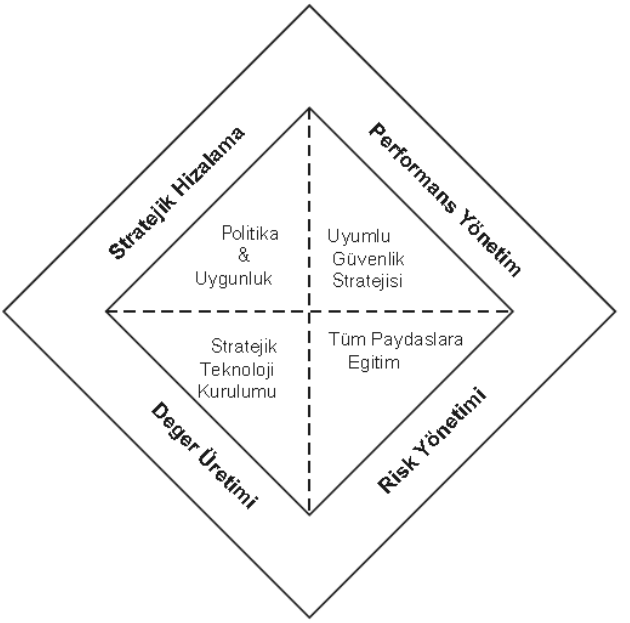


Şekil 9.5. COBIT-5 Yönetişim Hedefi
(Kaynak: Araştırmacılar tarafından oluşturulmuştur.)

BT yönetişimi, COBIT modeli üzerine bina edilmiş yeni bir model olup, kurumsal tüm süreçlerin elektronik ortamlarda ve elektronik tekniklerle bir biriyle uyum içerisinde olan yönetişimin kavramsal ifadesidir. Buna göre; risk yönetimi, stratejik yönetim, performans yönetimi, kaynak yönetimi ve hizmetlerin sunumu bir birinden ayrılmaz ve birbirine bağımlı tamamlayıcı süreçler olup hepsinin uyumlu yönetimine "*IT Governance*" denilmektedir. Bu alanın sürekli yeni kavram ve ifadelerle sürekli değişim göstereceği söylenebilir [18]. Bilişim yönetişimi konusu da aşağıda ayrı bir paradigma yaklaşımı olarak ele alınarak detaylı bir şekilde incelenmeye çalışılmıştır. Görüldüğü gibi yeni ortaya çıkan kavramlarla nesnesi etkilenen ve sürekli yeni gelişme ve icatlara sahne olabilen yönetişim alan ının sınırlarını belirlemenin bu anlamda zorlaşmakta olduğu söylenebilir.

BT yönetişimi (*IT Governance*), COBIT üzerine bina edilmiş ve BT Yönetişim Enstitüsü tarafından üretilmiş yeni bir model olup bir organizasyondaki tüm süreçlerin elektronik ortamlarda ve elektronik tekniklerle bir biriyle uyum içerisinde yönetişiminin kavramsal ifadesidir. Buna göre risk yönetimi, stratejik yönetim, performans yönetimi, kaynak yönetimi ve hizmetlerin sunumu bir birinden ayrılmaz birbirine bağımlı tamamlayıcı süreçler olup hepsinin uyumlu yönetimine *"IT Governance"* ifadesinin tercümesi olarak bilişim

yönetişimi denilmektedir. Burada bilişim ile yönetişimin birleştirilmesinden farklı bir paradigma üretildiği görülmektedir [41].



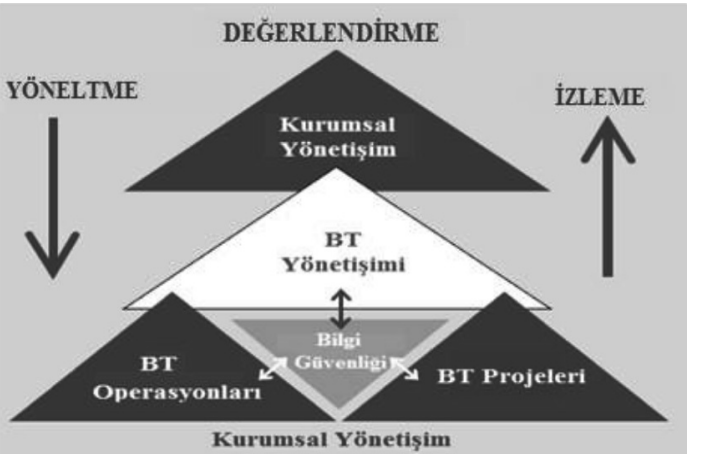
Şekil 9.6. BT Yönetişimi [41].

Kurumsal risk yönetimi ve katma değer elde etmede BT'nin merkezi rolünü dikkate aldığımızda son yirmi yıl içerisinde BT yönetişimi konusuna özel bir önem verilmektedir. BT yönetişimi kuşkusuz kurumsal yönetişimin tamamlayıcı bir parçasını teşkil etmektedir. Kurumsal BT yönetişimi, bir kurumdaki süreçlerin, yapıların ve ilişkisel mekanizmaların tanımlanmasını ve uygulanmasını ifade eder ki yönetim kurulları ile üst yönetimlerin BT yönetimi ile birlikte risk ve değer üretimi yönetimini destekleyecek şekilde sorumluluklarını yerine getirmeye olanak tanınsın [54].

BT yönetişimi konsepti, yirmi yıldan beri bilinmektedir. 1990'lı yılların başlarında BT yönetişiminin kilit taşları akademik alanda serpilmeye başlanmıştı. Bir boyutunda BT fonksiyonlarının farklı ve birbirine alternatif organizasyonları ile bunların iş sonuçları üzerindeki etkileri incelenmişti. Başka bir boyutunda BT fonksiyonunun organizasyonu ve bunun verdiği hizmetlerin, vatandaş/paydaş/ yararlanıcı konumundaki iş birimleri arasındaki eşgüdümün yapısı ve sonuçları çalışıldı. Üçüncü bir boyutunda ise daha çok kurumsal

stratejiler, BT yatırımları ve kurumsal performans arasındaki bağlantılar açıklanmaya çalışılmıştır [54].

İç Denetim Enstitüsü (IIA) tarafından üretilen bir kavram olarak da bilgi güvenliği yönetişiminden söz edilebilmektedir. Daha çok BT yönetişiminin bir alt dalı olarak ifade edilebilen bilgi güvenliği yönetişimi kavramı oldukça yenidir. Bilgi Güvenliği Yönetişimi, liderlik, kurumsal yapılar ve kurum bilgi teknolojilerinin sürdürülmesini ve kurum stratejilerini ve hedeflerini desteklemesini güvenceye alan BT projeleri, operasyonları ve yönetişimiyle ilgili süreçlerden oluşur [33].



Şekil 9.7. Bilgi Güvenliği Yönetişimi [33]

Yönetişim ile ilgili olarak pek çok yeni paradigmaların üretilebildiği ve bunların birbirilerinden etkilenerek sürekli farklı noktaları nazara verebilen yeniliklere girdikleri söylenebilir. Bilgi güvenliği yönetişimi de bu bağlamda, ulusal verilerin korunması ve merkez kapitalist ülkelere olan bağlılığın azaltılması açısından dikkatle ele alınması gereken bir konudur. Yenilikçi bilgi, üretken ve stratejik teknik bilgiler ile sektörel pazar payları, mali ve parasal işlemler, zafiyetler, kırılganlıklar, ulusal ve savunma sanayi ile ilgili projeler gibi kritik öneme sahip enformasyon ve bilginin korunmasını güvenceye alacak bir bilgi güvenliği yönetişim altyapısı büyük önem arz etmektedir. Ulusal, kurumsal ve kişisel bilgi güvenliği, yönetişim ilişkilerinin korunması ve illegal yapılanmaların etkisine girilmemesi açısından stratejik önemi haiz bir konudur.

Yeni teknolojiler, daha verimli süreçler ve daha iyi eğitimli personel ile bile, bazı şeylerin sunulması zorlaşıyor ve dikkate değer bir alan değer. İşletmeler, işe insanlar, süreçler ve teknolojiyle hizmet veren ve genellikle bu değeri hizmet biçiminde sağlayan birden fazla hizmet sağlayıcıdan oluşur. Bu iş için ne anlama geliyor? Değer, risk ve kaynakları optimize ederken, işletme faydaları elde etmekten oluşur. Hizmet sağlayıcılar tarafından sağlanan hizmetlerde değer olmadan işletmeler büyük olasılıkla paydaş değerinde ve daha da önemlisi iş hayatında büyük bir düşüş bekleyebilirler. Bu "değer" tanımındaki unsurlar daha fazla açıklanabilir:

- *Faydaların sağlanması*, işletmenin paydaş ihtiyaçlarına göre elde ettiği yeni faydaları elde ettiği ve düşük performans gösteren girişimleri veya varlıkları elimine ettiği anlamına gelir. Siber risklerin bunları ihlal etmemesi için stratejiler olmalıdır.
- *Risk optimizasyonu*, riske maruz kalma işletmenin risk iştahı dahilinde olduğunda bilgilendirilmiş işletme kararları vermenin sonucudur. Tüm risklere karşı tam güvence yaklaşımı kabul edilebilir olmadığı gibi aşırı maliyetli olacağından kurumun amaçlarına ulaşmasını ve paydaşların menfaatlerini elde etmelerini engelleyecektir.
- *Kaynak optimizasyonu*, kurumsal kaynakların doğru zamanda, yerde ve çabada uygulanmasını ve anlamsız bir şekilde boşa harcamamasını gerektirir. Kaynakların makul bir şekilde tahsis edilmesi gerektiği için operasyonla ile güvenlik arasında bir denge kurulmalıdır.

Genel olarak, başarılı inovasyon ve iş dönüşümünün anahtarı, bu değer unsurlarını maksimize eden genel bir yönetişim, risk ve kontrol (GRC) duruşunun bir parçası olarak, temel bir kolaylaştırıcı kümesine yatırım yapmayı gerektirir. Bir işletme GRC işlevlerinde güçlü yetkinlikler sergiliyorsa, rekabetçi kalmak ve bugünün ekonomisinde gelişmek için gereken dönüşümü sağlamak için iyi bir konumda olacaktır. Bu işlevlerin dönüşümsel hedeflere ulaşılmasındaki önemini göz önünde bulundurmamak, işletme tekerleklerini proaktif değil de reaktif bir modda döndürürken büyük hayal kırıklığına neden olabilir. Değer sağlama zorluğuna eklemek için, siber güvenliği girin. Paydaşlar birçok şeyden etkilenir ve bugünün

ortamında, siber güvenliğin büyük olasılıkla etkilenenler listesinin başında bir yerde olması muhtemeldir.

Basitçe ve rastgele bir şekilde çeşitli güvenlik mekanizmalarını uygulamak yeterli olmayabilir. Etkili olması için, güvenlik önlemlerinin işletme mimarileri ve GRC programlarına tam olarak entegre edilmesi gerekir. Siber güvenlik geleneksel olarak teknolojik bir sorun olarak düşünülmüş olsa da, siber güvenlik riski sadece teknik çözümlerle ele alınamaz. Pek çok ihlal, teknolojiye değil, politikalara, yönetim denetimine, siber güvenlik görevleri veya gözetimi için sorumluluk alamama ve kurumsal sistemlere ve verilere erişim için yetersiz kontroller sistemine atfedilebilir. Siber güvenlikte yönetişim, bu nedenle, aşağıdakileri içeren birkaç çaba gerektirir:

- Teknolojinin uygulanması
- Yönetimin gözetimi
- Yasal ve düzenleyici farkındalık
- Çalışan eğitimi
- Bilgi teknolojisi ortamını düzenleyen politika ve prosedürlerin benimsenmesi ve uygulanması

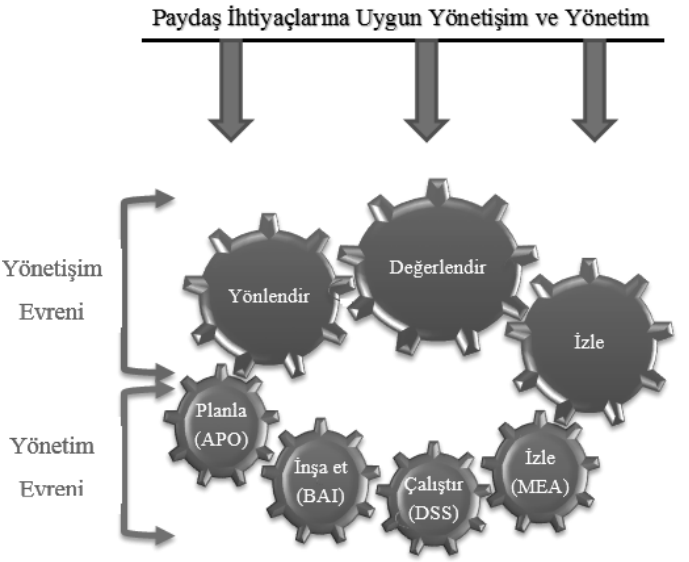
Bu gerekli çaba, genel kurumsal yönetişimin önlemleri ve riske yönelik tutumlar, kurumsal siber güvenlik programını yürütmelidir. Bu sürücüler, örgütsel davranış ve eylem kültürüne entegre edildiklerinde daha etkilidirler. Perspektifteki bu değişim, teknik bir kaygıdan bir işletme sorununa güvenliği artırıyor. Güvenlik kaygıları, paydaşların değer tanımını etkilediğinden, kuruluşun siber güvenlik tehditlerini tanımlamalı, korumalı, tespit etmeli ve bunlardan kurtarılmalı ve güvenlik riskinin stratejik hedefler, operasyonel kriterler ile yönetilmesi ve uyumlu hale getirilmesi için birçok temel kaynak ve yetkinliğe odaklanmalıdır [58].

Risk eşikleri, uyumluluk gereksinimleri ve teknik sistem mimarisi. Siber güvenlik, risk yönetimi ile ilgilidir. Risk yönetişimi ve yönetimi bilinçli karar verme ile ilgilidir. Bu nedenle, siber güvenlik denkleminin iki bileşeni vardır: iş olanakları ve varlık koruması. Öncelikle, siber güvenlik çabaları, işletme stratejisini sunarak kurumsal GRC çerçevesine uyacak şekilde hizalanmalıdır. Siber risk kritik bir iş riskidir ve dolayısıyla önemli bir unsurdur. İkincisi, bilgi önem-

li bir kurumsal varlıktır ve kritiklik, bütünlük ve kullanılabilirlik gereksinimlerine göre korunmalıdır. Siber güvenlik, işletme GRC kapsamının büyük resminde göz önünde bulundurulmalıdır, çünkü bugünün ekonomisindeki bilgilerin taşınması ihtiyacı başarı için hayati öneme sahiptir.

9.7. Yönetişim İle Yönetimin Ayrışması

COBIT-5 yaklaşımının diğer karakteristik özelliklerinden birisi de yönetim ve yönetişim arasında kesin bir çizgi koyarak ayırmasıdır. Bunun gerekçesi de yönetim ve yönetişim süreçlerinin, amaçlarının ve organizasyonel yapılanmalarının farklı olmasıdır. Buna göre yönetişim; paydaşların ihtiyaçlarının şartlarının ve seçeneklerinin dengeli ve uzlaşılmış kurumsal amaçların belirlenmesi için değerlendirilmesini, karar almada ve önceliklendirmede sevk ve idareyi belirlemeyi ve kurumsal amaçlar ve yönlendirmeye göre performans ve uygunluğu gözetlemeyi güvenceye alır. Özel yönetişim sorumlulukları kurumsal yapılanma, karmaşıklık ve imkânların elverdiği ölçüde bazı özel birimlere devredilebilir. Yönetim ise yönetişim organı tarafından yapılmış olan sevk ve yönlendirmeye göre planlama, inşa etme, yürütme ve gözetim işlevlerini yerine getirir.

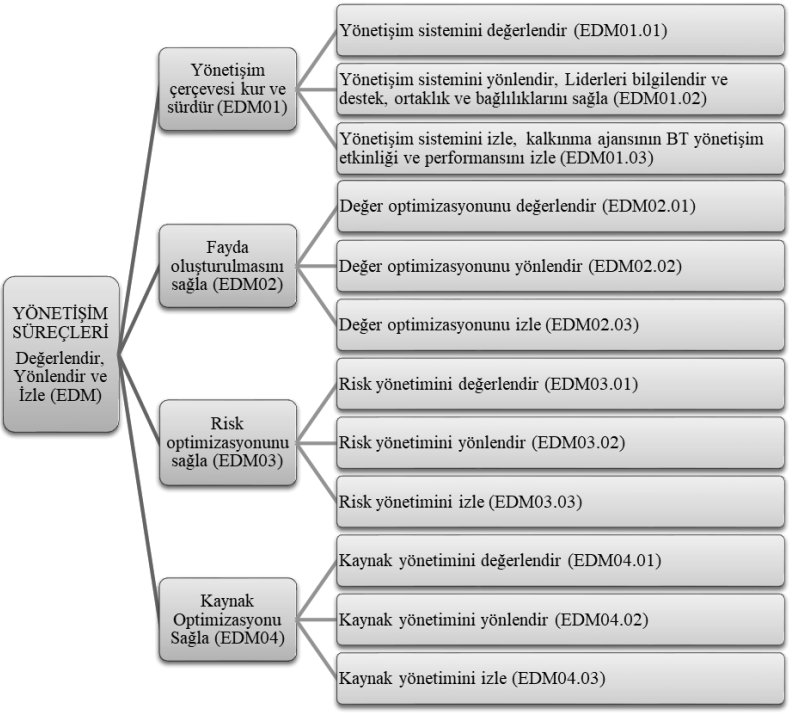


Şekil 9.8. COBIT-5 Yönetişim ve Yönetim Evrenlerinin Süreçlerde Ayrılması
(**Kaynak:** Araştırmacılar tarafından hazırlanmıştır.)

COBIT-5 süreç referans modeli, kurumların BT yönetişim ve yönetim süreçlerini, süreç etki alanları halinde bölümlere ayrılmış halde yönetişim ve yönetim olmak üzere iki ana faaliyet alanına ayırır. Yönetişim karar mekanizmalarını ilgilendirirken yönetim kararların uygulama mekanizmasını ifade etmektedir. Bu yaklaşıma göre her ikisi birbirinden girdi almalarına rağmen ayrışık olmaları gerekir. Çünkü karar mekanizması ile uygulama mekanizması kurumsal olarak aynı amaçlara hizmet ederlerken farklı niteliklere ve süreçlere sahip olmalıdırlar.

Yönetişim- Bu etki alanı beş yönetişim süreci içerir; her süreç dâhilinde EDM uygulamaları tanımlanır [26].

Yönlendir, değerlendir ve izle olarak belirlenen süreçler EDM olarak bilinmekte olup her biri üçer alt süreci olan dört ana süreçten oluşan bir çerçevedir. Süreçlerin nasıl uygulanacağı ve ölçüleceğine dair inceleme ileriki kısımlarda yapılacak olup bu kısımda kavramsal olarak Şekil 9.9'daki gibi gösterimi mümkündür.



Şekil 9.9. COBIT-5 Yönetişim Süreçleri Şeması
(**Kaynak:** Araştırmacılar tarafından hazırlanmıştır.)

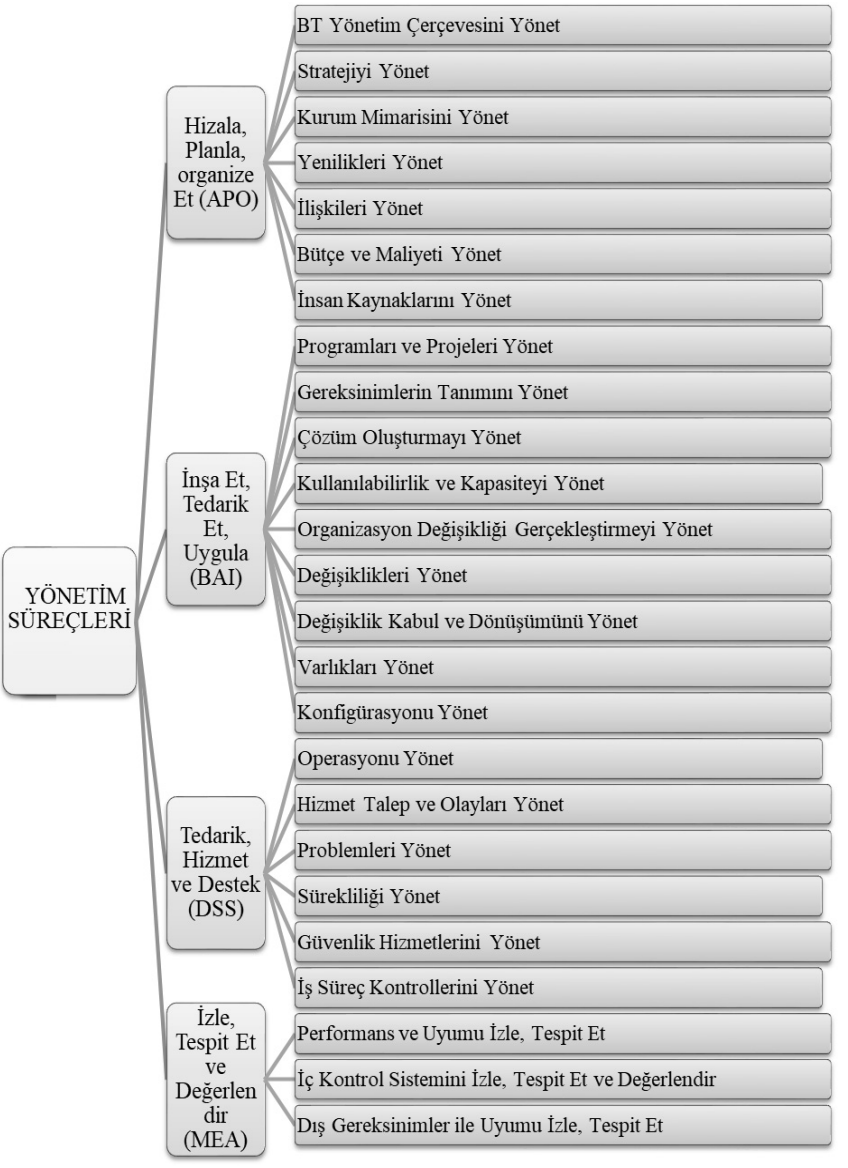
Şekil 9.9'dan anlaşıldığı üzere; yönetişim paradigmasının COBIT-5 ile geldiği noktada, yönetişim çerçevesi kurma ve sürdürme, yönetişim sistemini değerlendirme, yönetişim sistemini yönlendirme, liderleri bilgilendirme ve destek, ortaklık ve bağlılıklarını sağlama, yönetişim sistemini izleme, kurumun BT yönetişim etkinliği ve performansını izleme, fayda oluşturulmasını sağlama, değer optimizasyonunu değerlendirme, değer optimizasyonunu yönlendirme, değer optimizasyonunu izleme, risk optimizasyonunu sağlama, risk yönetimini değerlendirme, risk yönetimini yönlendirme, risk yönetimini izleme, kaynak optimizasyonu sağlama, kaynak yönetimini değerlendirme, kaynak yönetimini yönlendirme ve kaynak yönetimini izleme gibi süreçler yönetişim süreçleri olarak belirlenmiş ve bu süreçler mekanize teknik bilgi dâhilinde kritik faaliyetler ve Kilit Performans İsterleri belirlenerek oluşturulabilmektedir.

COBIT-5 çerçevesinde yönetişim ile yönetimin süreçler bağlamında birbirinden ayrıldığı görülmektedir. Bu teknik olarak süreçlerin işleyişinin profesyonel düzlemde tesis edilmesini sağlamak ve her iki sürecin girdi ve çıktılarının olabildiğince bir biriyle ilişki içerisinde ve tutarlı olmasını temin etmeye yöneliktir. Şekil 9.10'da yönetim alanında "*domain*" diye ifade edilen dört ana başlık ve bu başlıkların altındaki yönetişim ana süreçleri görülmektedir. Bu ana süreçlerin de en az 3 er tane alt süreci mevcuttur. Yönetim süreçlerinin bir kısmı yönetişim süreçlerinden aldığı girdilerle işleyebilmektedir.

Birçok kuruluş, faaliyetlerin beraberinde getirdiği olumsuz niyetlere eşlik eden siber tehdidi, özellikle risk yönetimi gündeminde öncelikli olmayan veya siber risk stratejisini oluşturmadan yaşamıştır. Siber tehditlere maruz kalmak artık yalnızca büyük çok uluslu şirketleri büyük veri merkezleriyle etkileyen bir şey değil. Siber tehditler, üzerinde çalışan ve Internet şebekesine bağlı olan herhangi bir kuruluş için geçerlidir. Neredeyse her zaman bir organizasyonu olumsuz yönde etkileyebilecek bir siber ihlal, artık; ne zaman meselesi olduğundan dolayı yönetim kurulları ve karar mekanizmalarının da müdahil olmalarını gerektirmektedir. Ancak bu alt ve orta ölçekteki yönetim birimlerinin müdahil olduğu şekilden farklı olmalıdır.

Bilgi ve teknoloji kullanımı ile gelen risklerle başa çıkmak için bir risk yönetimi açısından ne kadar hazır olduğunu. Bu, kurulun ve yürütme kurulunun toplantılarında öne çıkan ve sürekli bir gün-

dem maddesi midir? Bu soruların her birinin cevabı olumlu değilse, kurum daha sonra siber saldırı riskine ve işlerin her zamanki gibi devam etmesini sağlamak için gereken kadar çabuk iyileşememe riskine maruz kalır.



Şekil 9.10. Yönetim Ana ve Alt Süreçleri
(**Kaynak:** Araştırmacılar tarafından hazırlanmıştır.)

İşin sürekliliğini sağlamak için yönetim kurulları, organizasyonun risk yönetimi çerçevesinin siber risklere yönelik olmasını sağlamalıdır. Siber riskler tanımlanmalı, kuruluşun çevresi ile ilişkili olarak ölçülmeli ve siberlerle ilgili olayların etkisini en aza indirecek uygun önlemler alınmalıdır. Kuruluşun liderliği, bir siber saldırıdan kaynaklanabilecek olaylar için iş sürekliliği planlarının ve düzenlemelerinin yapılmasını sağlamalıdır. Siber risklerle uğraşmak artık yalnızca BT departmanındaki işletme personelinin sorumluluğunda değil. Siber tehditler, yönetim kurulunda ihtiyaç duydukları dikkat seviyesini ve üst düzey liderlik seviyelerini karşılayamayacak kadar büyüktür.

Siber güvenlik, risk yönetimi ve iş sürekliliği planlaması yönetim kurulunda ve yürütme komitesinin gündeminde sürekli yer almalıdır. Bu, boşlukların olabileceği alanlara uygun dikkat gösterilmesini sağlayacaktır. Bu şekilde, tespit edilen boşlukları ele almak ve riske maruz kalmayı en aza indirgemek için gerekli süreçlerin ve çözümlerin uygulanmasının ve ayrıca riskin işletmeye ve operasyonlara yönelttiği etkinin güvenceye alınmasına yönelik taahhüt sağlanmış olacaktır.

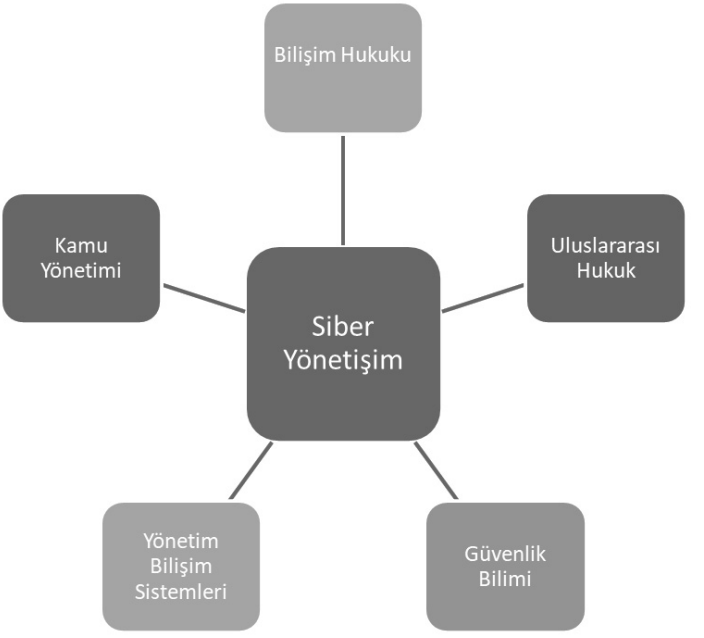
9.8. Siber Yönetişimde Uygulanabilir Ölçeklendirme

"*Siber yönetişim*", bilişim hukuku, kamu yönetimi, uluslararası hukuk, yönetim bilişim sistemleri ve güvenlik biliminin kesişiminde siber tehditlerin bertaraf edilmesi, siber risklerin yönetilmesi ve gerekli kontrol noktalarının ve politikalarının tesisinde kaynak ve değer optimizasyonunu gerektiren yeni bir yaklaşımdır.

Siber yönetim ile yönetişim farklıdır. Yönetişim karar alma ve katılım süreçleri ile ilgiliyle yönetim uygulama ve raporlama süreçlerini barındırır. Diğer bir değişle, yönetişim, sevk ve idareyi sağlayan mekanizma iken yönetim, icra ve eylem mekanizmasıdır. Şekil 9.11'de incelendiği üzere, yönetişim ile yönetim mekanizmalarının ayrışmasının gerektiği COBIT-5 çerçevesi ile ortaya atılan yeni bir paradigmadır.

Bazı araştırmacılar, siber güvenliği insan hakları kapsamında değerlendirebilmişlerdir. Örneğin bir çalışmada, [39] iyi siber yönetişimde, insan hakları tabanlı bir yaklaşım sergilemesi gerektiği daha fazla hesap verebilirlik, daha fazla şeffaflık ve daha fazla katılım sağlanması açısından savunulmuştur. Bunun yanı sıra iyi siber gü-

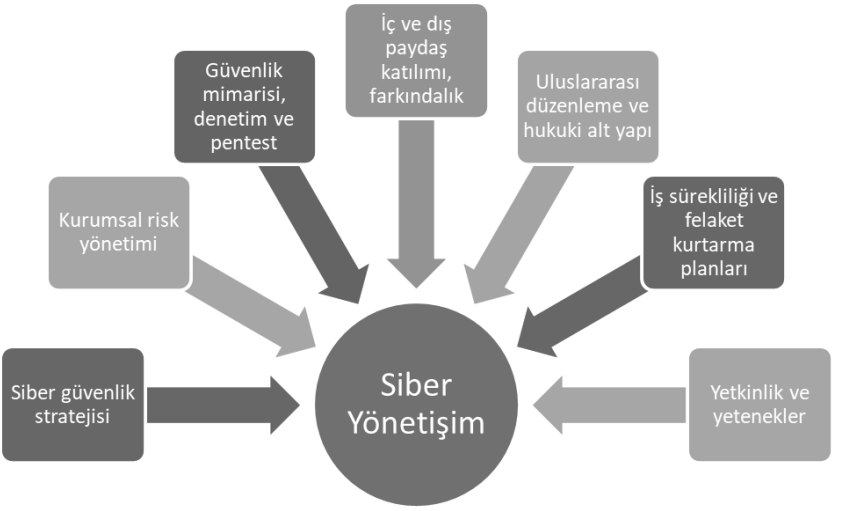
venliğin insan haklarını teknoloji üzerinden koruduğu da savunulmuştur. Siber alanın, vatandaşlık, milliyet ve politik köken veya cinsiyet ayırımı olmaksızın iletişim ve etkileşimin yapıldığı sınır tanımayan bir uzay olduğu bilinmektedir. Bireyler siber alanı, politika yapmak, gelir getirici faaliyet yapmak veya yaşamlarını kazanmak için internet üzerinden kullanmaktadırlar. Ancak bu alan ortak bir standart, yönetişim mekanizması, kontrol araçları ve kurallarıyla henüz güvenceye alınamamıştır. Küresel insan hakları kuralları ve standartları bu alanda rehberlik oluşturarak siber yönetişimi kurmak için kullanılabilir. Ulusal siber güvenlik stratejileri bu alanda siber yönetişimin kurgulanmasını sağlayacak en önemli araçlar olarak ortaya çıkmaktadırlar. Bu nedenle siber yönetişimin tesis edilmesi için ulusal siber stratejilerin olgunluğu, uygulanabilirliği ve yetkinliği önem arz etmektedir.



Şekil 9.11. Siber Yönetişimin İlgili Olduğu Disiplinler
(**Kaynak:** Araştırmacılar tarafından hazırlanmıştır.)

Siber yönetişim ise siber alanla ilgili önlemleri almada katılımcılık, şeffaflık ve hesap verebilirliği arttıracak şekilde karar alma süreçlerinin işletilmesini gerektirir. Siber yönetişim için öncelikle bir ulusal strateji olmalı, kurumsal risk yönetimi, kurumsal güvenlik mimari-

si, güvenlik denetimi sızma testleri, düzenleme ve sertifikasyon, iş sürekliliği planları ile siber güvenlik ile ilgili yetkinlik ve yeteneklerin mevcut olması gerekir. Bu bileşenler ve aynı zamanda gerekliliker Şekil 9.12'de verilmiştir.



Şekil 9.12. Siber Yönetişim Bileşenleri & Gereklilikleri
(**Kaynak:** Araştırmacılar tarafından hazırlanmıştır.)

Öncelikle 2016-2019 Ulusal Siber Güvenlik Stratejisi eylem başlıkları, bilişim hukuku ile uluslararası hukuk kapsamında değerlendirilerek ayrıştırılmış ve COBIT-5 BT yönetişimi kapsamında analiz edilmiştir. Tablo 9.1'de bu noktada yapılan değerlendirme görülmektedir.

Tablo 9.2'den görüleceği üzere, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının Bilişim Hukuku, Uluslararası Hukuk ve COBIT-5 ile değerlendirilmesi yapılabilmektedir. Bu kapsamdaki değerlendirmelere siber yönetişim gereklilikleri dikkate alındığında katılımın geniş tutulması, özel sektör ve sivil toplumu da kapsaması ve paydaş ihtiyaçlarını dikkate alan kaynak-ihtiyaç dengesini gözeten bir strateji hazırlanması gerektiği söylenebilmektedir.

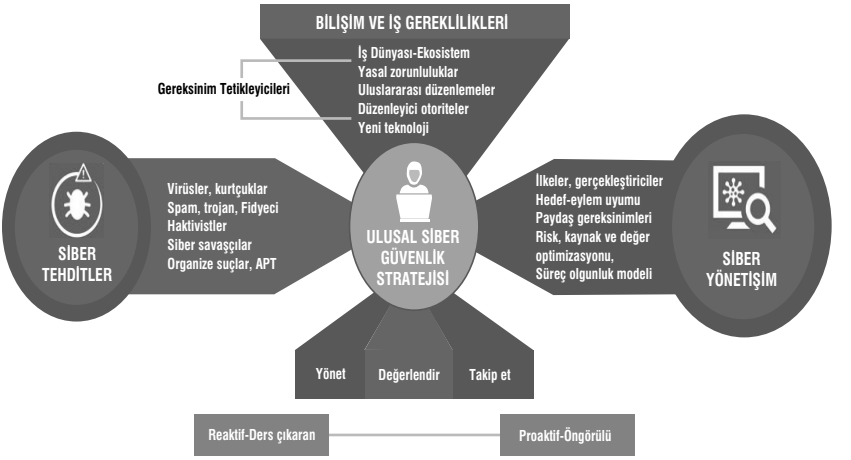
Tablo 9.1. 2016-2019 Ulusal Siber Güvenlik Stratejisi Eylem Planının Bilişim Hukuku, Uluslararası Hukuk ve COBIT-5 ile değerlendirilmesi **(Kaynak:** Araştırmacılar tarafından hazırlanmıştır.)

Stratejik Eylem Başlığı	*Bilişim Hukuku*	*Uluslararası Hukuk*	*COBIT-5 BT Yönetişimi*
1. Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması	Bu konuda birincil mevzuat çalışmalarının tamamlanması ve iletişim güvenliğinin sağlanmasına yönelik güvenlik esaslarının oluşturulması alt eylemleri mevcuttur.	Birincil mevzuat kapsamında uluslararası hukuk ile ilgili düzenlemeler de yer almalıdır.	SOME iş tanımları, 27001 ve pentest zorunluluğu, siber güvenlik yönetim süreci ve güvenlik esaslarının belirlenmesi kabul edilebilir ve gerekli eylemlerdir. Süreçler ve KPI göstergeler yok. Sorumlu, bilgilendirilen, danışılan ve hesap veren belli değil.
2. Siber Suçlarla Mücadele	Ceza ve yargılama mevzuatının düzenlenmesi, adli analiz kapasitesinin geliştirilmesi, adli uzman havuzu ve kriterleriyle ilgili eylemler mevcuttur.	İlgili ceza ve yargılama mevzuatı düzenlemeleri kapsamında uluslararası hukuk ile ilgili gereklilikler ve sorumluluklar da dikkate alınmalıdır.	Mevcut durum analizi, IPv6 kullanımı ve büyük veri analizi altyapısının kurulması kabul edilebilir ve gerekli eylemlerdir. Paydaş ihtiyaçlarının tespiti yapılmalıdır. Süreçler ve KPI göstergeler yok. Sorumlu, bilgilendirilen, danışılan ve hesap veren belli değil.
3. Farkındalık ve İnsan Kaynağı Geliştirme	Bilişim hukukçusu yetiştirilmesi, ilk-orta-yükseköğretim müfredatında siber güvenlikle ilgili içerik sağlanması ile ilgili eylem mevcuttur.	Uluslararası işbirliğinin güçlendirilmesi ile ilgili eylem mevcuttur.	Gerekli insan kaynağı potansiyelinin sağlanması ve farkındalığın arttırılması ile ilgili yeterli düzeyde eylem mevcuttur. Süreçler ve KPI göstergeler yok. Sorumlu, bilgilendirilen, danışılan ve hesap veren belli değil.
4. Siber Güvenlik Ekosisteminin Geliştirilmesi	Denetleme ve sertifikalandırma mekanizmalarının oluşturulması, firma envanteri çıkarılması, yerli teknoloji ve ürünlerin geliştirilmesi ve ulusal iş modeli oluşturulması ile ilgili eylemler mevcuttur.	Uluslararası hukuk değerlendirilmelidir. NATO Tallinn Rehberine göre ekosistem geliştirilmelidir.	Laboratuvar ve test yapısı, güvenlik ortamı, Pardüs kullanımı ve güvenli yazılım kültürü ile ilgili eylemler mevcuttur. Ekosistem ile ilgili olarak paydaş ihtiyaçları tespit edilmelidir. Süreçler ve KPI göstergeler yok. Sorumlu, bilgilendirilen, danışılan ve hesap veren belli değil.
5. Siber Güvenliğin Milli Güvenlikle Entegrasyonu	Eylemler net değil.	Eylemler net değil.	Süreçler ve KPI göstergeler yok. Sorumlu, bilgilendirilen, danışılan ve hesap veren belli değil.

Tablo 9.2. Siber yönetişimde paydaş aktörler ile eylemlerin eşleştirilmesi (**Kaynak:** [27]' den esinlenen araştırmacılar tarafından hazırlanmıştır.)

Aktörler	Eylem				
	Kural Geliştirmeye katkı	*Kuralların yayılması ve uygulanması*	*Hafif kurallara uyum sağlama*	*Uluslararası yükümlülüklere uymaya rıza*	*Yükümlülükleri yasal olarak uygulatmak*
DEVLETLER	√	√	√	√	√
ULUSLARARASI ORGANİZASYON (BM, AB, vb.)	√	√	√	√	
ÖZEL SEKTÖR	√	√	√		
SİVİL TOPLUM	√	√	√		
TEKNİK (Üniversite, Enstitü vb.)	√	√	√		

Devlet, kamu kurumları ve uluslararası organizasyonlar için geçerli olan pek çok durumun aslında özel sektör paydaşları, sivil toplum ve teknik insanlar veya organizasyonlar açısından geçerli olmayabileceği söylenebilir. Aktörlerin siber yönetişimdeki durumlarının ve tavırlarının dikkate alınması gerekir ki etkili bir siber güvenlik stratejisi hazırlanabilsin.



Şekil 9.13. Ulusal Stratejide Siber Yönetişim Modeli (**Kaynak:** Araştırmacılar tarafından oluşturulmuştur.)

Sadece hizmete özel ve sorumlu olan kamu kurumlarına imza karşılığı verilen bir stratejinin ne derece kapsayıcı, şeffaf ve tüm aktörlerin ihtiyaçlarını dikkate alabileceği değerlendirilmelidir. Şekil 9.3'deki aktörler ile siber güvenlik ile ilgili süreçler ve gerekliliklere göre takındıkları durumlar gösterilmektedir.

Şekil 9.13'de kısaca gösterildiği üzere bir siber güvenlik stratejisi öncelikle iş dünyası, ekosistem, yasal zorunlulukları, uluslararası düzenlemeler, düzenleyici otoriteler ve yeni teknolojik gelişmeler tarafından tetiklenmelidir. Bu kapsamdaki siber yönetişim de belirli ilkeler ile gerçekleştiricilere sahip olmalı, ortaya konulan hedeflere ulaştıracak uygulanabilir eylemlerle desteklenmeli, iç ve dış paydaş gereksinimlerini dikkate almalı, kurumların risk, kaynak ve değer optimizasyonunu belirli bir süreç olgunluk modeli üzerine bina etmelidir. Bu siber yönetişim sistemi belirli tehditleri bertaraf ederken yönetilebilir, değerlendirilebilir ve takip edilebilir bir süreç modeline sahip olmalıdır. Bu süreçlerin izleme mekanizması da ders çıkarıcı ve öngörülü olmalıdır.

Önleyici siber güvenlik önlemleri tek başına değerli bilgi varlıklarınızı koruyamaz. Güvenlik duvarları ve oturum açma protokolleri iyi bir ilk savunma hattıdır. Ancak ihlaller kaçınılmaz olarak gerçekleşecek. Onlar ne zaman korunuyorsunuz? Artan bir ihlal yüzdesi içeriden kaynaklanan tehditler nedeniyle, siber güvenlik riskini çevrenizde etkin bir şekilde yönetmenin yollarını geliştirmelisiniz.

- Yukarıdan aşağı doğru siber tehditleri yönetmek için bütünsel ve dinamik bir yol haritası geliştirin
- Mevcut uygulamaların etkinliğini analiz etmek ve güvenlik açıklarını belirlemek
- Teknik güvenlik konularını önemli iş paydaşlarının kavrayabileceği şartlara dönüştürmek
- Müşterilere ve yatırımcılara gereken özeni gösterme - ve güven aşılama
- Tüm BT ve iş uygulamaları için politikayı merkezi olarak yönetin
- Tüm BT ve iş uygulamalarınızda işlevler arasında risk ve uyumluluk gereksinimlerini birleştirin ve siber güvenlik prosedürlerini standartlaştırın.

- Siber standartları iç kontroller ve işlemler ile hizalayın ve vizyonunuzu ve sorunların çözülmesiyle ilgili ilerlemenizi açıkça belirtin.
- Siber güvenlik çerçevelerinin, yetkilerin ve yönetmeliklerin ve ilgili değişim yönetimi süreçlerinin alımını otomatikleştirin
- Tüm BT ve iş uygulamalarınızda siber güvenlik prosedürlerini standartlaştırın.
- Siber tehditler, içeriden öğrenen riskler ve veri ihlallerini analiz edin ve istisnaları iş koluna göre kontrol edin
- İş etkilerine göre müdahale ve iyileştirme faaliyetlerini önceliklendirin
- Sorunun bir siber saldırı olamayacağı bir zamanda güvenlik pozisyonunuzun iş paydaşlarına güvence verin, fakat ne zaman gerçekleşeceği hususunda senaryolar ve bunlara göre önlemler belirleyici olacaktır.

9.9. Siber Güvenlik Yönetişimi Çerçevesine Olan İhtiyaç

Bugünün önerileri, çalışma biçimleri, düşünce biçimleri ve çalışma biçimleri üzerinde büyük bir değişim geçiriyor. Bu değişim, tüm BT endüstrisini etkileyen büyük teknolojik (bulut ve mobil), entelektüel (büyük veri ve analitik) ve davranışsal (sosyal) dönüşümlerle bastırılıyor. Güvenlik de bu devrimden etkilendi. Aslında, değişimin kendisinden daha fazla, güvenliğe olan etki, gelişmelerin hızından kaynaklanmaktadır.

Örgütsel sınırların azalmasıyla birlikte güvenlikteki zorluklar büyüyor ve bir işletme içindeki daha fazla departman ayarlamalardan etkileniyor. Bugün örgütler izole edilmiş silolar olarak işlev göremezler. Değişimi benimsemeleri ve kendilerini İnternet'in ve ilgili teknolojilerinin engin, çeşitli ve güvensiz dünyasına açmaları gerekiyor [33].

Daha güçlü ve daha yaygın siber güvenlik tehditlerinin ortaya çıkması ile birlikte, örgüt liderleri siber uzayda bekle ve izle modunda olamazlar. İnternetin açık ekosistemi siber suçlulara muazzam bir güç sağlıyor ve siber güvenliği teknik bir problemden daha fazla yapıyor - bu bir iş problemi. Gerçekleşen bir tehdidin potansiyel sonuçları oldukça geniştir ve bu da siber güvenliği toplantı salonuna sürüklemiştir [39].

Bir siber güvenlik çerçevesi aslında bir dizi yönetim aracı, kapsamlı bir risk yönetimi yaklaşımı ve daha da önemlisi, kurumdaki herkesi baştan aşağı kapsayan bir güvenlik bilinci programı olmasıdır. Başka bir deyişle, her organizasyonun tüm siber güvenlik ihtiyaçlarını tam olarak ele almak için eksiksiz bir siber güvenlik yönetişim çerçevesine sahip olması gerekir. Bu güvenlik duruşunu şekillendirmede önemli rol oynayan ve bu nedenle uzun vadeli başarı için kritik öneme sahip birkaç kilit bileşen vardır. Bu bileşenler şunlardır:

- Örgütsel yapı,
- İş kültürü,
- Güvenlik bilinci programları ve
- Siber güvenlik yönetişimidir.

Bu özelliklerin her biri, güvenlikteki boşlukları kapatmak için diğerleri ile birlikte çalışır. Belirli bir ihtiyaç alanına odaklanmak bir fark yaratabilirken, en etkili girişimler işletmeyi korumak için bu bileşenlerin dördünü de kullanacaktır.

9.9.1. Organizasyon Yapısı

Kuruluşun nasıl yapılandırıldığı ve güvenlikle ilgili girişimleri nasıl yönlendirdiği, güvenlik duruşunun tanımlanmasında ve şekillenmesinde önemli bir rol oynamaktadır. Kurumsal yapı içinde iyi tanımlanmış bir güvenlik ve uyumluluk yönetimi zinciri bu çerçevenin temel bileşenlerinden biridir. Yalnızca yönetimin güvenlik sorunlarına katkıda bulunmak için daha uygun olmasını sağlamakla kalmaz, aynı zamanda kuruluşun bu nedenle ne kadar odaklandığını da gösterir.

9.9.2. İş Kültürü

Kuruluş içindeki iş kültürü nedir? Bu, ekiplerin bilgi güvenliğine nasıl baktıklarını ve hızla değişen örgütsel değişikliklere nasıl tepki verdiklerini içerebilir. Bunlar siber güvenlik kültürünün oluşumu için hayati öneme sahiptir. Geleneksel çalışma yöntemleri ve kurum içindeki veya dışındaki çeşitli paydaşlarla etkileşimin değişen manzaraya göre ayarlanması gerekir.

9.9.3. Güvenlik Bilinci

Çalışanlar neyin doğru neyin yanlış olduğunu bilmiyorsa, güvenlik söz konusu olduğunda, istenmeyen tuzaklara düşme ihtimalleri çok daha yüksektir. Güvenlik uyumluluğuna ilişkin politikaları oluşturmanın geleneksel yaklaşımının yanı sıra, kuruluşların tarafsız bir şekilde farkındalık ve eğitim programlarına odaklanması gerekir. İşletmeler, işgücünü çalıştıkları ekosistemden haberdar kılma konusundaki taahhütlerini ve ciddiyetlerini göstermek için bir politikaya ihtiyaç duyarlar.

9.9.4. Siber Güvenlik Yönetişimi

Yönetişim, sadece mevcut ihtiyaçlar için değil aynı zamanda gelecekteki zorluklar için iyi hazırlanmış hafifletme planları yapılmasında da organizasyonun güvenlik hedefine ulaşılmasında son derece önemli bir rol oynamaktadır. Mevcut sorunları ele almak için, yönetişim çerçevesi güvenlik politikalarındaki iyileştirmeleri kapsar; teknik kontrollerin uygulanması; denetimler ve değerlendirmeler; ve insanlar arasında bilinçli davranışların güvenli davranışlara karşı tutumlarını şekillendirmelerini sağlamaktır. Gelecekteki zorluklar için, yönetişim çerçevesi sürekli olarak ortaya çıkan tehdit faktörlerine, teknolojik peyzajdaki hızlı hareket eden değişikliklere, insanların görüş ve davranışlarına ve iş kültürü dönüşümlerine odaklanmalıdır [41].

Bugün, siber tehditler her köşeden kurumlara nüfuz ediyor. Çalışanlar tarafından kullanılan uç noktalardan, BT altyapısını veya iş operasyonlarını yönetmek için kullanılan araç ve uygulamalardan veya bulut manzaralara yayılmış farklı bileşenler arasındaki bağlantıdan kaynaklanıyor olsanız da, her yerde risk var. Bu risk faktörlerinin büyük bir kısmı örgütsel hizmetleri veya varlıkları işleten, yöneten ve hatta kullanan kişilerle ilgilidir. Bu, her organizasyonda iyi tanımlanmış bir siber güvenlik çerçevesini gerekli kılar ve çoğu işletme BT ve işletme ekosistemleri için bir tane oluşturmak için ciddi çaba sarf eder.

9.10. Yöneticilerin Dikkate Almaları Gereken Siber Yönetişim Temel Soruları

Kurumların, halka açık şirket yöneticilerinin, şirketlerinin siber güvenlik çerçevesini incelerken sorması gereken bazı temel sorular:

- Yönetim kurulunun hangi kısmı siber güvenlik risklerinin incelemesini üstlenmelidir? Bütün Kurul mu olmalı? Bu sorumluluk Denetim Komitesine mi verilmeli? Özel siber güvenlik tecrübesine sahip ilave Kurul üyeleri işe alınmalı mı?
- Yönetim kurulu (veya Komite) ne sıklıkla siber güvenlik brifingleri almalıdır? Işık hızında hareket eden ve günlük olarak siber ihlallerin bildirildiği bu dünyada, üç aylık brifingler yeterli mi? Kurul, siber güvenlik ile ilgili aylık brifing almak zorunda mı?
- Birçok siber güvenlik sorununun karmaşıklığı ve büyüklüğü göz önüne alındığında, Kurul siber güvenlik konularında istişare etmek ve kurumun üst yönetimi, CISO, CTO ve CIO tarafından yapılan uygulamalarla ilgili soru sormak için kendi "siber danışmanlarını" işe almalı mı?
- Kurumun en değerli siber varlıklarına yönelik en büyük tehdit ve riskler nelerdir? Kurumun beşeri ve finansal sermayesi, bu yüksek değerli varlıkları korumakla aynı hizada mı?
- Kurumun haftalık veya aylık bazda siber olay hacmi nedir? Bu olayların büyüklüğü / ciddiyeti nedir? Bu olaylara cevap verme süresi ve maliyeti nedir?
- En kötü siber olayla ilgili olarak kuruma iş kaybı olarak ne zarar verir?
- Kurumun belirli siber olay planı nedir ve müşterilere, müşterilere, satıcılara, medyaya, düzenleyicilere, kanun uygulayıcılara ve hissedarlara nasıl yanıt verecektir?
- Kurum çalışanlarına hangi siber güvenlik eğitimi verilmelidir?
- Kurum, üçüncü taraf hizmet sağlayıcıları ve satıcıları için ne tür bir "siber durum tespiti" yapıyor?
- Şirket birleşmeleri ve devralmalar bağlamında, herhangi bir devralmanın dikkate alınması kapsamında yapılan siber durum tespiti düzeyi nedir?
- Kurum, bilgisayar korsanlarının yararlanabileceği olası güvenlik açıklarını analiz etmek için Kurumun ürün ve hizmetlerinin "siber sağlamlığı" konusunda bir analiz yaptı mı?

- Ulusal Siber Güvenlik Stratejisindeki gerekli eylemler gerçekleştirilebildi mi?
- Son olarak, Kurum, tamamen veya kısmen NIST siber güvenlik çerçevesini, Kurumun IP varlıklarını korumak için olumlu eylemler göstermenin bir yolu veya yöntemi olarak benimsemeli midir?

Kuşkusuz bu listede verilen hususların sayısı artabilir. Ancak, amacına hizmet ettiğine inandığımızdan, üst yönetim ve üst düzey BT personeli hakkında sorulması gereken en önemli hususları dahil etmeye çalıştık. Çözülmesi gereken sorular risk yönetimi yaklaşımına göre en önemliden itibaren dikkate alınmalıdır. Bu soruların ağırlığı da her kurumun iç kontrol sistemi, risk yönetimi ve yönetişim yapısına göre değişkenlik gösterebilir. Ayrıca, yöneticilerin zorlu soruları değerlendirmek, sormak ve çözümlemek noktasındaki gözetim görevlerini yerine getirmelerine yardımcı olmak için iç denetçilerin bilgisine, danışmanlarına ve alan profesyonellerine ihtiyaç duyabilirler.

9.11. Değerlendirmeler

Siber alan, teknik, ekonomik, politik, sosyal, askeri, kolluk kuvvetleri ve akıllı alanlardaki tartışmaları kapsamaktadır. Siber uzayın yönetimi, geniş bir kurallar, normlar, kurumlar ve süreçler kümesi olarak görülebilir. Siber uzay, askeri açıdan Kara, Hava, Uzay ve Deniz ile eşit bir alan adıdır (örneğin: Savaş İlkeleri'nin temel sorularını uygulayın). Siber yönetişim, devlet davranışları ve devlet dışı aktörler için resmi ve gayri resmi normların oluşturulmasını, sınır ötesi siber suçları ele almanın daha iyi yasal mekanizmalarını, yasaların uygulanması için şeffaf ulusal mevzuatı ve verilerin bütünlüğünü korumak için şifreleme ihtiyacının onaylanmasını içermektedir.

Zamanın geçmesiyle ve insanlığın artık sanal gerçeklikle büyüyen IoT denilen nesnelerin interneti ile daha fazla bütünleşmesiyle siber ortamdaki risklerin yönetilebilir olması ve aktörlerin kendi rolleri hakkında yeterli bilgi sahibi olması aciliyet kesp etmektedir. Bazı ülkeler çevrimiçi güvenlik ve siber hijyen için eğitim programları yapmakta ve bunları müfredatına yedirmektedir. Aynı zamanda vatandaşlar da neyin güvenilir olup olmadığını anlayabilmeli ve

internet üzerinden yapılan kara propaganda ve yanlış yönlendirmelere karşı uyanık olmak zorundadır. Siber yönetişim bunu gerektirmektedir. Sadece planlar, politikalar ve teknik önlemler yetersiz kalmaya mahkûm olmaktadır. Planlar özellikle birbirileriyle uyum içerisinde olmalı ve uluslararası çerçeve ve standartlara uygun bir şekilde hazırlanmalıdır. Çevrim içi ve çevrim dışı mevcut bilginin değerlendirilmesi ve anlaşılması çok önemli yetkinlik haline gelmiştir. Bu yetkinliklerin kazanılması da çocukluktan itibaren örgün ve yaygın eğitimi de kapsayacak şekilde kapsamlı bir eğitim ve öğretim programıyla olanaklıdır.

Soğuk savaş yıllarında ABD ile SSCB arasında bir nükleer savaş çıkma olasılığı tüm dünyayı yakından alakadar eden büyük tahribat oluşturabilecek bir risk ile ilgili merak ve endişe konusuydu. Şimdilerde ise Çin ile ABD arasında ekonomik ve askeri alandaki rekabet ve mücadele siber ortama da taşınmıştır. Çoğu ülke artık siber ordular oluşturmakta ve karşılıklı saldırılarda bulunabilmektedir. Bazı siber savaşçılar ise haktivist veya bağımsız hacker görünümünde bazen onları da kullanarak uluslararası hukuk kapsamına girecek müdahalelerde bulunabilmekte ve ulusal egemenliği ve vatandaşlık haklarını ihlal edecek saldırılar düzenlemektedirler. Bu nedenle de NATO tarafından yayınlanan TALLINN Rehberinde görüleceği üzere sadece ulusal mevzuat değil aynı zamanda uluslararası hukuk da büyük önem arz etmektedir. Dolayısıyla siber yönetişim sadece bireysel, kurumsal, yerel, ulusal, bölgesel değil aynı zamanda küresel bir algıyı ve katılımı gerektirecek ölçüde önemli bir konu haline gelmiştir. Yakın bir gelecekte siber silahlarla gerçekleştirilebilecek saldırıların, sonuçları açısından klasik savaşları aratmayacağı ve elektrik santrallerinin devre dışı bırakılması, nükleer santrallerin kontrollerinin ele geçirilerek potansiyel birer atom bombasına dönüştürülmesi, basıncın artırılarak doğal gaz borularının havaya uçurulması, baraj kapakları açtırılarak şehirlerin sular altında bırakılması, iletişim ağlarının devre dışı bırakılmasıyla haberleşmenin sekteye uğratılması ve hava, kara ve deniz trafiğinin aksatılması gibi sonuçlar doğuracağı beklenmektedir.

Bu bölüm kapsamında yapılan araştırma ve incelemelerden sonra araştırma sorularımız aşağıdaki şekilde cevaplanabilmektedir:

9.11.1. Siber alanı kimler yönetmelidir?

Siber alan sadece kişisel verilerin değil, kurumsal ve ulusal verilerin tehdit altında olduğu bir sanal evrendir. Siber tehditler sanal alanda paylaşılan verilerin hacim ve nitelik olarak artması ve bulut bilişim olanaklarının yaygınlaşmasıyla birlikte teknolojinin zafiyetlerinden yararlanma ve suiistimal etme şeklinde tezahür etmektedirler. Bu sanal alanda öncelikle bireyle kendi verilerini tehdit eden risklere karşı gerekli bilgi ve duyarlılık ile donatılmalı, kurumsal gerekli personel imkânları ve sertifikasyonlarla güçlendirilmeli ve uluslar da aktif ve pasif siber savunma yapabilen yetkin ekipler, yasan düzenlemeler ve kurumsal yapılarla ulusal hükümranlıklarını ve vatandaşlarının hak ve özgürlüklerini koruyacak stratejilere sahip olmalıdırlar. Bireyler, kurumlar ve ulusların sanal alandaki tehditlere karşı ayrı ayrı görevleri vardır. Her şey sadece devlet, mahkemeler ve kurumlardan beklenemez. İnsan unsuru ve bilinç düzeyi her zaman ön plandadır. Siber alanın yönetilmesinde uluslararası işbirlikleri ve ulusüstü kurumların düzenlemelerine uyum sağlanması da büyük önem taşır. Ayrıca, Ar-Ge ve yenilikçi teknolojilerle başkanlarının sahip olmadığı teknik ve yöntemlerin geliştirilmesinde öncülük edenler siber alanda her zaman üstün olacaklardır.

9.11.2. Siber alan yasal (formel) ve yasadışı (informel) alanda nasıl yönetilmelidir?

Resmi alanda, yasa ve yönetmelikler ile yapılan düzenlemeler uluslararası kurallarla uyumlu bir şekilde icra edilebilmeli ve bunun için gerekli olan kurumlar arası işbirliği ve görev ayırımı doğru bir şekilde yapılabilmelidir. Görev karmaşası, yetki çatışması bazı sorumlulukların ortada kalmasına veya yetersiz bir şekilde icra edilmesine neden olabilir. Yasal alanda "siber yönetişim" bir kaçınılmaz gereklilik olarak karşımıza çıkmaktadır. Kaynakların, risklerin ve değerlerin bireysel, kurumsal ve ulusal ölçekte optimize edilmemesi durumunda stratejiler ve eylemler etkin bir şekilde işlemeyecektir.

Yasadışı alanda ise yeraltı örgütlenmeleri, mafya ve taşeron terör grupları çalışmaktadır. Bunlara karşı en etkili yöntem bunları takip ederek zararlarını minimize edecek ve gerektiğinde aktif savunma ile bertaraf edebilecek siber orduların kurulması ve kurumsal ölçekte ise siber güvenlik uzmanları istihdam etmektir.

Bilişim hukuku, medeni hukuk ve uluslararası hukuk kapsamında ifade edilen risklerin makul düzeyde güvenceye alınabilmesi ve siber saldırılara karşı etkin mücadele sürecinde hak ihlallerinin ve telafisi zor zararların meydana gelmemesi için öncelikle anılan strateji ve eylemler için güçlü bir izleme ve değişim yönetimi sisteminin sürdürülmesi gerektiği düşünülmektedir. Bu kapsamda aşağıdaki önlemlerin de dikkate alınmasında yarar görülmektedir:

1. Siber güvenlik konusuna ilişkin silahlı çatışma hukukunun ötesinde yeni ve ayrı bir dal olarak, siber saldırı ve savunma konularının tanımları dâhil tüm detayları da kapsayacak "Siber Güvenlik Hukuku" adıyla yeni bir dalın oluşturulmasına yönelik çalışmaların yapılmasının uygun olacağı değerlendirilmektedir.
2. Tehditlere karşı koruyucu pasif savunma alanında yapılanların yanında aktif savunmaya (offensive security) da yönelik tedbirler alınmalıdır. Siber güvenlik alanında tedbirler geliştirirken güvenlik-demokrasi, fayda-maliyet dengelerinin gözetilmesi gerektiği gözden kaçırılmamalıdır.
3. Siber saldırgan veya teröristlerin milliyet ve aidiyetlerinin tespit edilmesinin güçleşmesi ve siber alanın ulus ötesi yapısı bu hukuku uluslararası hukukun düzenlemesine bırakmasından dolayı ulusal normlar dışında uluslararası siber hukuk ile ilgili TALINN Rehberi ve anlaşmalara uyum sağlamaya özen gösterilmesi daha isabetli olacaktır.
4. "*Siber yönetişim*" gerekliliklerinin COBIT-5 modeli çerçevesinde dikkate alınarak tüm ulusal stratejileri kurumsal stratejilerle kaynakların imkân verdiği ve beşeri sermayenin elverdiği ölçüde hizalanmaya çalışılmalı, kurumsal ve profesyonel yönetim anlayışları bu paralelde geliştirilmelidir.
5. Kurumsal politika ve uygulamaların olgunluğu ve yeterliliği kuşkusuz üst düzey yönetimlerin etkisini belirleyen *"the tone at the top"* denilen algı ve yaklaşımları ile biçimlendiğinden dolayı, daire başkanı ve üstü görevlere atamada bilişim alanında belirli bir ölçüde yetkinlik istenmesi, yetkinliği olmayanların belirli eğitimlere tabi tutulmaları ve uzman düzeyindeki görevliler için de uluslararası ölçüde kabul görmüş CSX, COBIT-5, CISA, CRISC gibi sertifikasyonların teşvik edilmesi siber yönetişim açısından büyük önemi haizdir.

Kaynaklar

[1] Akbulut, Y. (2015). Yeni Nesil Akran Zorbalığı-Siber Zorbalık. *Bilişim Hukukunun Güncel Sorunları Konferansı.* Eskişehir: Anadolu Üniversitesi Hukuk Fakültesi.

[2] Albayrak, G. (2013). Siber Alan ve Uluslararası Hukuk: Siber Savaş Çağı. *www.academia.edu/2504279/Siber_Alan_ve_Uluslararası_Hukuk.*

[4] Al-Rawi, A. K. (2014). Cyber warriors in the Middle East: The case of the Syrian Electronic Army. *Public Relations Review*, 420-428.

[5] Altıparmak, K. (2015). Evrensel İnternetten Türk Tipi İnternet'e: İnternet Sansür Ağı. *Bilişim Hukukunun Güncel Sorunları Konferansı.* Eskişehir: Anadolu Üniversitesi Hukuk Fakültesi.

[6] Arabacı, M. (2015). Google Glass, Mahremiyet ve Türk Ceza Kanunu. *Bilişim Hukukunun Güncel Sorunları Konferansı.* Eskişehir: Anadolu Üniversitesi Hukuk Fakültesi.

[7] Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. *Security Strategies Journal*, p119-147.

[8] BKK, B. K. (2013, 02 18). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.* Resmi Gazete: http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm adresinden alınmıştır.

[9] BKK, B. K. (2016, 08 10). *2016-2019 Siber Güvenlik Ulusal Stratejisi.* Ulaştırma Bakanlığı: http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf adresinden alınmıştır.

[10] Crawford, J. (2012). *Brownlie's Principles of Public International Law.* 8th edition: Oxford.

[11] Çakır, H., & Kılıç, M. S. (2013). Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış. *Polis Bilimleri Dergisi*, 23-44.

[12] Çelik, Ş. (2014). Stuxnet Saldırısı ve Abd'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi.*

[13] Çetin, H. (2014). Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi. *Akdeniz İ.İ.B.F. Dergisi*, 86-105.

[14. Dawson, J. (1998). Institutions, investment, and growth: New cross-country and panel data evidence. *Economic Inquiry Vol. XXXVI, October*, 603-619.

[16] Doğru, M. (2015). Siber Harekatın Uluslararası Hukuk Çerçevesinde Analizi. *http://ab.org.tr/ab16/bildiri/106.pdf.*

[17] Dülger, M. V. (2004). Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler. *İstanbul Barosu Dergisi*, 1485–1496.

[18] Efe, A. (2016). Bilişim Hukuku Alanındaki Sorunlar ve Risklerin Mevzuat Boyutuyla Analiz ve Çözümlemesi. *TNB Hukuk Dergisi, http://www.tnb.org.tr/tnbonlineekler/HukukDergisi/YIL3/SAYI1/index.html#p=182*, 175-200.

[20] Efe, A. (2017). Siber Suçlar ve İhlallerde Kamu Otoritesinin Sorumluluğu Üzerine Bilişim Hukuku ve Uluslararası Hukuk Kapsamında Bir Analiz. *TNB Hukuk Dergisi*.

[21] Efe, A., Uzunay, y., & Taşcıoğlu, g. (2009). An eGovernment Information System Framework:Turkish National Agency Software Project. *eTransformation in Public Administaration: From eGovernment to eGovernance* (s. 110-125). ANTALYA: TODAİE, SESRIC, UNDP.

[22] Finnkle, J. (2014). *North Korea Surfaces in Sony Investigations Probe into Hack.* http://www.reuters.com/article/us-sony-cybersecurity-investigation-nkor-idUSKCN0JH28920141204: Routers.

[23] Güler, M., & Ömürgönülşen, U. (2011). Türkiye'de e-İmza Alanındaki Hukuki Düzenlemeler. *Sosyoekonomi*, 198-230.

[25] Heinegg, W. H. (2005, Vol. 48). The United Nations Convention on the Law of the Sea and Maritime Security Operations. *German Yearbook of International Law*, 151-185.

[26] Hekim, H., & Başıbüyük, O. (2012). Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*.

[27] Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 135-158.

[34] Henkoğlu, T., & Külcü, Ö. (2013). Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme. *Bilgi Dünyası*, 62-86.

[38] Henkoğlu, T., & Uçak, N. Ö. (2012). Elektronik Bilgi Güvenliğinin Sağlanması ile İlgili Hukuki ve Etik Sorumluluklar. *Bilgi Dünyasi*, 377-396.

[39] ISACA. (2012b). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows, IL: ISACA.

[40] Jayawardane, S., Larik, J., & Jackson, E. (2015). *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance.* The Hague Institute.

[42] Kaynak, S., & Koç, S. (2015). Telif Hakları Hukuku'nun Yeni Macerası: Sosyal Medya. *folklor/edebiyat*, 389-411.

[43] Koruyan, K., & Bingöl, F. I. (2015). Bulut Bilişim Hizmet Sağlayıcılarının Veriyi Koruyamamaları Durumuyla İlgili Türk, Avrupa Birliği ve Amerikan Hukukundaki Düzenlemeler. *9 eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 367-388.

[44] Kurnaz, İ. (2016). Siber Güvenlik Ve İlintili Kavramsal Çerçeve. *Cyberpolitik Journal.*

[47] Külcü, Ö., & Turan, M. (2013). Kamu Hukukunda Geleneksel ve Elektronik İletişim, Bilgi ve Belge Yönetimi Uygulamaları. *Türk Kütüphaneciliği*, 266-300.

[48] Küzeci, E. (2015). Kişisel Verilerin Korunması Alanındaki Güncel Gelişmeler. *Bilişim Hukukunun Güncel Sorunları Konferansı.* Eskişehir: Anadolu Üniversitesi Hukuk Fakültesi.

[50] Lewis, P. M., & House, C. (2017). *Global Cyber Governance in 2017: Information Integrity.* https://www.cfr.org/councilofcouncils/global_memos/p39008.

[51] Lotrionte, C. (2012). *State Sovereignity and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights.* EMORY INT'L.

[52] Love, P., Reinhard, J., Schwab, A., & Spafford, G. (2006). *GTAG Global Teknoloji Denetim Rehberi Bilgi Güvenliği Yönetişimi.* ABD: IIA-TİDE.

[53] Margulies, P. (2013). Sovereignty And Cyber Attacks: Technology'S Challenge To The Law Of State Responsibility. *Melbourne Journal of International Law*, p496-519.

[54] Mavzer, Ş. (2016, 01 10). *Siber Suçlarla Mücadelede Uluslar Arasi İşbirliği (International Cooperation Against Cybercrime).* cybercrimesmavzer.blogspot.com.tr: http://cybercrimesmavzer.blogspot.com.tr/2014/11/siber-suclarla-mucadelede-uluslar-arasi.html adresinden alınmıştır

[55] Memiş, T. (2015). Hukuki Açıdan Verilerin Ticarileştirilmesi. *Bilişim Hukukunun Güncel Sorunları Konferansı, 20 Mart.* Eskişehir: Anadolu Üniversitesi Hukuk Fakültesi.

[56] Mihr, A. (2014). Good Cyber Governance: The Human Rights and Multi-Stakeholde Approach. *Georgetown Journal of International Affairs International Engagement on Cyber IV*, 24-34.

[58] Miynat, M., & Duramaz, S. (2013). Karapara Aklama Aracı Olarak Yeni Bir Mali Suç: Siber-Aklama. *Journal of Management & Economics*, p.315-325.

[59] Moeller, R. R. (2013). *Executive's Guide to IT Governance.* New Jersey: John Wiley & Sons, Inc.

[60] Moore, S. (2013). Cyber Attacks and the Beginnings of an International Cyber Treaty. *North Carolina Journal of International Law & Commercial Regulation*, p223-257.

[61] Öğün, M. N., & Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Security Strategies Journal*, 145-181.

[62] Önok, M. (2013). Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslar Arası İşbirliği. *Marmara Üniversitesi Hukuk Araştırmaları Dergisi*, 1229-1270.

[63] Özkan, H. (2015). Sosyal Medya Aracılığıyla İşlenen Suçlar. *Bilişim Hukukunun Güncel Sorunları Konferansı.* Eskişehir: Anadolu Üniversitesi Hukuk Fakültesi.

[64] Palmer, B. (2012). How Dangerous Is a Cyberattack? *Slate*, http://www.slate.com/articles/news_and_politics/explainer/2012/04/how_dangerous_is_a_cyberattack_.html.

[65] Payne, T. (2016). Teaching Old Law New Tricks: Applying And Adapting State Responsibility To Cyber Operations. *Lewis & Clark Law Review.*, 683-715.

[66] Percoco, M. (2011). Geography, institutions and urban development: Italian cities, 1300–1861. *Springer-Verlag*, 135-152.

[67] Perlroth, N. (2014). Sony Pictures Computers Down for a Second Day After Network Breach. *New York Times*.

[68] Pirker, B. (2001). Territorial Sovereignty and Integrity and the Challenges of Cyberspace. K. Ziolkowski içinde, *Peacetime Regime for State Activities in Cyberspace* (s. 189, 208). Estonia: CCDCOE.

[69] Sanger, D., Schmidt, M., & Perloth, N. (2014). *Obama Vows a Pesponse to Cyberattack on Sony.* New Yok Times.

[70] Schmitt, M. N. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*,14-37.

[73] Schmitt, M. N. (2014). Rewired warfare: rethinking the law of cyber attack. *International Review of the Red Cross*, 189–206.

[74] Steven De Haes, W. V., & Roger, S. D. (2013, Spring). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal Of Information Systems, 27*(1).

[75] Turan, M., & Külcü, Ö. (2014). Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi. *Türk Kütüphaneciliği*, 18-46.

[76] USOM. (2016, 01 20). *Siber Olaylara Müdahale Ekipleri Kurulum Adımları*. www.usom.gov.tr: https://www.usom.gov.tr/duyuru/2015/01/siber-olaylara-mudahale-ekipleri-kurulum-adimlari.html adresinden alınmıştır

[77] Ünsal, B. (2015). Arama Motorlarının Sorumluluğu ve İnternet Hukuku. *Bilişim Hukukunun Güncel Sorunları Konferansı, 20 Mart.* Eskişehir: Anadolu Üniversitesi Hukuk Fakültesi.

[78] Wedutenko, A. (2015). Cyber attacks: Get your governance in order. *Governance Directions*, p598-601.

[79] Yıldız, S. (2002). Internet Servis Sağlayıcılar ve Cezai Sorumlulukları. *Selçuk Üniversitesi İktisadi ve İdari Bilimler Fakültesi Sosyal ve Ekonomik Araştırmalar Dergisi*, 167-184.

[80] Yıldız, S. (2007). Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 209-623.

[82] Ziolokowski, K. (2013). *Tallin Mannual on Peacetime Regime for State Activities in Cyberspace.*

Siber Savaş ve Siber Silahlar

BÖLÜM 10

Hatice TOMBUL

SİBER SAVAŞ VE SİBER SİLAHLAR

Bu bölümde, siber savaş ve siber silahlar hakkında bir literatür çalışması verilmiştir. Gelişen teknolojiler sebebi ile ülkelerin savunma ihtiyaçları gün geçtikçe artmakta ve ülkelerin saldırı ve savunma yapmak amacıyla geliştirdikleri savaş yöntemleri ve silah sistemleri de oldukça karmaşık hale gelmektedir. Özellikle bilişim alanında hız kazanan gelişmeler neticesinde, siber savaş ve siber silahlar gibi siber güvenlik kavramları da literatüre hızla girmeye başlamıştır. Siber savaş, aktörlerin silahlı bir çatışmaya gerek duymadan hedeflerine ulaşabilecekleri bir strateji olarak tanımlanabilmektedir. Siber silahlar ise; sistemler üzerinde izleme yapabilme, bilgi toplayabilme veya istenilen sistemleri çalışamaz hale getirebilme yeteneğine sahip herhangi bir yöntem veya araç olarak tanımlanabilmektedir. Siber silahların maliyetleri düşük olmasına karşın etki alanları oldukça yüksektir. Siber silahlarla gerçekleştirilecek siber savaşların yapacağı etkilerin de en az geleneksel savaşlardaki kadar yıkıcı ve öldürücü olacağı bir gerçektir. Bu çalışma kapsamında, siber savaş ve siber silah kavramları hakkında bilgi verilmiş, siber silahların kavramsal tasarım modeli ile yaşam döngüsünden bahsedilmiş, hedef odaklı, arkasında büyük destekler olan popüler siber silahlar incelenerek hedeflenen sonuçlara ne kadar ulaşabildikleri değerlendirilmiş ve ülke olarak almamız gereken önlemler belirtilmiştir.

10.1. Giriş

Günümüzde gelişen teknolojinin etkisiyle, ülkelerarası anlaşmazlıklar ve çıkar çatışmaları şekil değiştirmektedir. Ülkeler arasındaki bu güç savaşları internet üzerine taşınmış ve ülkeler birbirlerine ekonomik, politik ve askeri alanlar gibi birçok alanda zarar verebilmek için siber uzayda organize saldırılar yapmışlardır. Siber uzay, birbiriyle bağlantılı sistem, yazılım, donanım ve insanların etkile-

şimde bulundukları soyut veya somut küresel bir alan olarak ifade edilmektedir. Siber uzay, birçok ülkede kara, hava, deniz ve uzay gibi bir askeri harekât alanı olarak kabul edilmeye başlamıştır. Siber uzayın en önemli unsuru internet olmasına rağmen, siber uzay iletişim ağları, elektronik komuta sistemleri, cep telefonları, uydu sistemleri gibi birçok sistem ve donanımı da kapsamaktadır. Bir ülkenin, hedef olarak seçtiği herhangi bir ülkeye siber uzayda gerçekleştirdiği organize saldırılar siber savaş olarak isimlendirilmiştir. Siber savaş, geleneksel savaşlara benzememekle birlikte kilometrelerce uzak mesafelerden düşmana ciddi hasarlar verebilmektedir. Siber savaşlar, sistemleri çalışamaz hale getirilebilme, kişisel bilgileri çalabilme, uçakları havada çarpıştırabilme, bankaları çalışamaz hale getirebilme, şehirleri elektriksiz bırakabilme, sahte belgelemeler yapılabilme, itibar kayıpları yaşatabilme gibi çeşitli hasarlara sebep olabilmektedir. Günden güne siber ortama kayan bu savaş alanı sebebiyle silahlar da isim değiştirmiş ve siber ortamda kullanılarak karşı tarafı etkisiz bırakmak veya zarar vermek gibi sebeplerle kullanılacak olan siber silahlar ortaya çıkmıştır. NATO Güvenlik Danışmanı Rex Hughes'in "Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır" sözü siber silahın geleceğini açıkça ortaya koymaktadır [1-3].

Dünyanın önde gelen silahlı kuvvetleri siber uzaya, siber savaşa ve siber silahlara uyum sağlayabilmek için çalışmalarını sürdürmektedirler. 2013 yılında Türk Silahlı Kuvvetleri de önemli bir adım atarak bünyesindeki Siber Savunma Merkezi'ni bir Siber Komutanlığa dönüştürmüştür. Günümüzde, Türkiye'nin siber savaş ve silahlar konusunda oldukça fazla yol alması gerekmektedir. Bu sebeple akademi, kamu ve özel sektörün siber savaş ve siber silah konularında ciddi işbirliği yapmaları gerekmektedir [4].

10.2. Siber Güvenlik

Siber savaş ve siber silah kavramlarından bahsetmeden önce bilgi, teknoloji ve siber güvenlik kavramlarından bahsetmek iyi olacaktır. Bilgi ve teknoloji kavramları birbirlerini tetikleyen iki kavram olarak düşünülebilmektedir. Bir başka deyişle, ülkelerin teknolojileri geliştikçe bilgi artışı olmakta, bilgi artışı oldukça da teknolojileri gelişmektedir. Bilgi, oldukça basit gibi görünse de düşmanların eline geçmesi halinde ciddi zararlara sebep olabilecek, korunması gere-

ken kritik bir kavramdır. Örneğin bir devletin askeri, mali bilgileri veya Ar-Ge projesi bilgileri, şirketlerin yatırım bilgileri, bireylerin özel iletişim bilgileri oldukça önemli bilgilerdir. Gelişen teknolojiler sebebiyle bu bilgilerin birçoğu internet ağları üzerinden erişilebilir durumdadır. Bu bilgilerin, kötü amaçlı kişiler tarafından internet üzerinden ele geçirilmelerini engellemek için önlemler alınması gerekmektedir. Siber uzayda, kullanıcıların, kurum ve kuruluşların, devletlerin varlıklarını ve kaynaklarını korumak amacıyla kullanılan tüm politikalar, teminatlar, araçlar, faaliyetler veya uygulamalar siber güvenlik olarak isimlendirilmektedir. Günümüzde, ülkelerin iyi ordulara sahip olmaları güvenlikleri için yeterli olmamakta, teknolojinin gelişmesiyle birlikte siber güvenliklerini de sağlamaları gerekmektedir [5]. Bunun için ülkelerin belli siber güvenlik yaklaşımları belirlemeleri, bunları belirlerken de bazı unsurları dikkate almaları önerilmektedir. Bu unsurlar Tablo 10.1'de açıklamalı olarak verilmiştir [6].

Dünyada siber güvenliğin sağlanması için çalışmalar her geçen gün artarak devam etmekte, bir yandan da siber tehditlere karşı siber savunma hazırlıkları yapılmaktadır. Siber savunma hazırlıklarının temel bölümü siber tehdit seviyelerinin belirlenmesidir ve bir sonraki bölümde ele alınmıştır.

10.3. Siber Tehdit Seviyeleri

Teknolojinin gelişmesine bağlı olarak siber tehditlerin de şekli değişmektedir. Önceden plansız siber saldırılar yapılırken, günümüzde organize ve arkasında büyük desteklerin bulunduğu siber saldırılar gerçekleşmektedir. Siber tehditlerin seviyeleri 1.seviyeden 5.seviyeye doğru ele alınmış ve aşağıda açıklamalı olarak verilmiştir [7, 8].

Siber Vandalizm: Kurumların itibarlarını zedelemek ve organizasyon yapılarına zarar vermek amacıyla küçük saldırgan gruplar tarafından gerçekleştirilmektedir.

Siber Hırsızlık/Suç: Kâr elde edebilmek, siyasi veya ideolojik amaçlara ulaşabilmek gibi sebeplerle bireysel şekilde ya da küçük saldırgan gruplar tarafından gerçekleştirilmektedir.

Siber İnfaz/Gözetleme: Siber kaynakları elde etmek, büyük saldırılar için gerekli verileri elde etmek gibi sebeplerle büyük saldırgan gruplar veya profesyonel suç örgütleri tarafından gerçekleştirilmektedir.

Tablo 10.1. Siber Güvenlik Unsurları

Siber Güvenlik Unsuru	Açıklaması
Ulusal politika ve stratejinin geliştirilmesi	Siber güvenlik çalışması yapan tüm bireylere, kurum veya kuruluşlara yol gösterecek ulusal bir politika ve bu politikaya dayanan bir strateji oluşturulması gerekmektedir.
Yasal çerçevenin oluşturulması	Siber suçların açıkça tanımlandığı, saldırganlar açısından caydırıcılığı yüksek olan hukuki düzenlemelerin yapılması gerekmektedir.
Teknik tedbirlerin geliştirilmesi	Yazılım, donanım ve iş süreçlerinin kalitesinin arttırılması, çeşitli güvenlik standartlarının oluşturulması ve uygulanması gerekmektedir.
Kurumsal yapılanmanın belirlenmesi	Asıl görevi siber güvenliği sağlamak olan kurumların, sorumluluklarının ve paydaşlarla ilişkilerinin yasal olarak açıkça belirtilmesi gerekmektedir.
Ulusal işbirliği ve koordinasyonun sağlanması	Günümüzde farklı paydaşlarca kullanılan sistemler ve altyapılar olduğundan, güvenliğin tam olarak sağlanabilmesi için tüm paydaşlar arasında işbirliğinin ve koordinasyonun sağlanması gerekmektedir.
Kapasitenin geliştirilmesi	Gelişen teknolojiye bağlı olarak siber tehditler, araçlar ve yöntemler de değiştiğinden, uygulama geliştiricilerin, hukukçuların, yönetim birimlerinin de teknolojiyi takip ederek kendilerini güncellemeleri gerekmektedir.
Farkındalığın artırılması	Son kullanıcı olan vatandaşların, siber tehditler, yöntemler ve riskler konusunda bilgilendirilmeleri ve farkındalıklarının arttırılması gerekmektedir.
Uluslararası işbirliği ve uyumun sağlanması	Küresel ağ üzerinden gerçekleştirilen ve tüm dünya ülkeleri için tehlike olan siber tehditlerin en aza indirilebilmesi için ülkeler arası hukuki mevzuatların uyumlu hale getirilmesi ve bilgi paylaşım mekanizmalarının oluşturulması gerekmektedir.

Siber Sabotaj/Casusluk: Ülkelerin özel programlarına erişmek için profesyonel istihbarat örgütleri tarafından gerçekleştirilmektedir.

Siber Savaş: Hedefin kritik bilgi altyapısını yok etmek amacıyla arkasında büyük destekler olan terörist gruplar tarafından gerçekleştirilmektedir. Bu çalışmanın temel konularından olan siber savaş kavramı takip eden paragraflarda ayrıntılı olarak ele alınmıştır.

10.4. Siber Savaş

Savaş kavramı neredeyse insanlık tarihinin başlangıcına kadar uzanan, insanlık tarihi ile aynı yaşta kabul edilebilecek bir kavramdır. Çok eski çağlardan beri savaşın tanımı üzerinde durulmasına rağmen herkesin kabul ettiği ortak bir savaş tanımı henüz bulunmamaktadır. Literatürde savaş ile ilgili olarak, inceleme alanlarına ve olaya bakış açılarına göre çok sayıda farklı tanım bulunmaktadır. Bu tanımlardan en sık karşılaşılanlarından birkaçı burada verilecektir. M.Ö. 400-320 yıllarında Çinlilerin tarihteki en ünlü başkomutanlarından Sun Tzu, oldukça popüler olan Savaş Sanatı adlı kitabında savaşı "yaşam veya ölümle son bulan bir sahadır ve hayatta kalmaya veya mahvolmaya giden bir yoldur" şeklinde tanımlamıştır. Carl Von Clausewitz'e göre savaş "politik ilişkilerin başka araçların desteği ile yürütülmesi" şeklinde ifade edilmiştir. Bir diğer popüler savaş tanımı ise Quincy Wright'a aittir. Ona göre savaş, "siyasal gruplar ve devletlerarasında belli bir sürede ve belirli büyüklükte silahlı güçlerle yürütülen çatışmalar" şeklindedir. Uluslararası hukukçular ve diplomatlar Grotius'un "güç kullanarak savaşanlar arasındaki durum" şeklindeki savaş tanımını kabul etmektedirler. Türkiye Cumhuriyeti ise, 2941 sayılı Seferberlik ve Savaş Hali Kanunu'nda savaşı tanımlamıştır. Bu kanuna göre savaş, "Devletin bekasını temin etmek, milli menfaatleri sağlamak ve milli hedefleri elde etmek amacıyla, başta askeri güç olmak üzere devletin maddi ve manevi tüm güç ve kaynaklarının hiçbir sınırlamaya tabi tutulmadan kullanılmasını gerektiren silahlı mücadeledir" şeklinde tanımlamıştır [9-13].

Tarihsel olaylardan bahsedilirken değinilmeden geçilemeyecek konulardan bir tanesi olan savaş, tarih boyunca hayatın her alanında ortaya çıkan değişimlerden etkilenmiştir. Orta Çağ döneminde, savaşta kullanılacak araç gereçler ilkel olduğundan ve coğrafi bilgi yetersizliğinden savaşlar kısa sürerdi. Bu dönemde hücum taktikleri

içeren savaş stratejilerini uygulamak önemliydi. Barutun keşfedilmesi ile İstanbul'un fethi sırasında topların kullanılması, savaş kavramında değişikliklere sebep olmuş ve yeni bir çağ açmıştır. Savaş tekniklerindeki bu değişiklik Yeni Çağ'da yeniden şekillenmiş ve Yeni Çağ'da uzaktan atılabilen silahlar ile modern tekniklere uyum sağlanmaya başlanmıştır. 1740-1815 dönemleri arasında geçen sürede de yeni savaş usülleri geliştirilerek savaş kavramında değişimler olmuştur. 1792 yılından itibaren sınırlı savaştan sınırsız savaşa geçiş olmuştur. Yani önceki dönemlerde savaşanlar ile sivillerin yaptıkları işler birbirinden farklıyken, Birinci Dünya Savaşı'nın ilk yarısından sonra savaş toplumlar arası bir mücadele şekline dönüşmüş ve sınırlı olmaktan çıkmıştır. Savaş ortamı, Orta Çağ dönemi öncesine göre sonrasında oldukça zorlaşmaya başlamıştır. Modern savaşlarda, toplar, tüfekler, savaş gemileri, tanklar gibi araçlar kullanılmaya başlanmıştır. Modern Çağda, bilgi, sermaye ve teknolojideki gelişmelerle birlikte savaş bambaşka bir yapıya bürünmeye başlamış, devletler geleneksel anlamda savaş girişimlerinden uzak durmuşlar ve modern tekniklere odaklanmışlardır. Modern çağ ile birlikte, siber savaş ulusal fiziki varlığa yönelmiş bir tehdit olarak ortaya çıkmıştır. Siber savaşların yapacağı etkilerin en az geleneksel savaşlardaki kadar yıkıcı ve öldürücü olacağı bir gerçektir [10, 13].

Siber savaş kavramı günümüzde birçok alanda karşımıza çıkmaya başlamış olmasına rağmen, bu konunun uzmanları tarafından bile kavramsallaşma sürecini henüz tamamlayamamış, uzlaşılan yanıtlar bulunamamıştır. Siber savaş, aktörlerin silahlı bir çatışmaya gerek duymadan hedeflerine ulaşabilecekleri bir strateji olarak tanımlanabilmektedir. Siber savaş, hedef ülkenin bilgisayar sistemlerine, haberleşme sistemlerine, enerji ve ulaşım ağlarına, askeri kontrol sistemlerine veya diğer hedef sistemlerine zarar verecek ölçüde yapılan bir savaş çeşididir. Siber savaş çok problemli hatta tehlikeli bir kavramdır. Bir savaş eylemi, siber uzayda olsun ya da olmasın araçsal, politik ve potansiyel olarak ölümcül olmalıdır [1, 4, 14].

Bu zamana kadar gerçekleştirilmiş olan bazı önemli siber savaş denemeleri bulunmaktadır. Bu bölümde, siber savaş örneklerinin bazılarından kronolojik olarak kısaca bahsedilecektir. Örneğin, 1999 yılında Kosava krizindeki taraf devletlerin NATO eposta hesaplarına, DDOS saldırıları gerçekleştirilerek devletlerin e-posta erişimleri uzun süre engellenmiştir. Bundan bir yıl sonra 2000 yılında,

Pentagon, NASA ve Birleşik Devletler Enerji Bakanlığı ve araştırma laboratuvarı bilgisayarlarına, Rusya merkezli olduğu ifade edilen saldırılar düzenlenmiş ve on binlerce dosyaya erişilmiştir. 2001 yılında, Dünya Ticaret Merkezi ve bazı diğer noktalara birçok insanın hayatını kaybetmesine sebep olan saldırılar gerçekleştirilmiş ve bu saldırılar ABD istihbarat örgütleri fark etmeden siber dünya üzerinden planlanıp koordine edilmiştir. Bu olay ABD açısından siber savunma zafiyeti olarak değerlendirilmiştir. 2003 yılında, ABD'nin Ohio kentindeki nükleer santrale Slammer isimli bir virüs ile saldırı düzenlenmiş, bu virüsün yaklaşık 8800 bilgisayara bulaştığı tespit edilmiştir. Saldırı sebebiyle sistem 5 saat duraksamış, bu duraksama ciddi maddi kayıplara sebep olmuştur. 2004 yılında Ulusal Ajans, Kore Savunma Enstitüsü gibi kurumlara Çin kaynaklı kötü niyetli programlar yüklenerek sistemlere zarar verilmiştir. Bundan yaklaşık iki yıl sonra 2006 yılında, iki ABD kongre üyesinin ofis bilgisayarları ele geçirilmiş ve bilgisayarlardan Pekin rejimi muhaliflerin bilgilerinin çalındığı düşünülmektedir. Aynı yıl ayrıca Malezya hafif raylı sistemlerine saldırı yapılmış, raylı sistemin bilgi sistemine hasar verilmiştir. 2007 yılında, Estonya ile Rusya arasında yaşanan gerginlikte, Estonya devlet kurumlarına, bankalarına, radyo ve televizyon istasyonlarına ait internet sunucularına DDOS saldırılarda bulunmuşlar ve bu sunucular bazı siber savaşçılar tarafından ele geçirilmiştir. Bu saldırının nereden koordine edildiği tespit edilememiş, Rusya tarafından gerçekleştirildiği tahmin edilmiş ancak ispat edilememiştir. 2008 yılında, ABD'de bilgisayar korsanları elektrik nakil sistemine saldırıda bulunarak elektrik kesintilerine sebep olmuşlardır. Bu sebeple ülkede birçok kişinin etkilendiği mağduriyetler yaşanmıştır. Aynı yıl Rusya ile Gürcistan arasında yaşanan savaşlar sırasında Rus korsanlar Gürcistan devletine karşı DDOS saldırıları yapmışlardır. Rusya, ülkedeki resmi kuruluşların finans ve basın-yayının bütün iletişimini üç hafta süreyle kesintiye uğratmıştır. 2008 yılında Rusya ayrıca ABD'ye yönelik bir siber saldırı da yapmıştır. Virüslü bir hafıza kartı yardımı ile ABD'nin savaşlarını yürüten komuta merkezine sızmış, bu sızıntının nerelere kadar ulaştığı tespit edilememiştir. 2009 yılında, ABD'de bir firmaya sahte yağ sızıntısı ihbarı yapılarak müdahale sistemleri aktifleştirilmiş ve firmada maddi kayıplara sebep olmuştur. Aynı yıl, Çinli korsanlar MS Windows'a ait açıklıklardan faydalanarak enerji sistemlerine

yönelik saldırı gerçekleştirmişlerdir. Bundan yaklaşık bir yıl sonra 2010 yılında, Çin merkezli olduğu belirlenen ve Google firmasının fikri mülkiyet haklarını çalmak üzere Auroa adı verilen bir saldırı yapılmıştır. Aynı yıl İran'ın nükleer tesislerine Stuxnet adlı virüs ile büyük ve uzun soluklu bir saldırı yapılmıştır. Belirli bir hedef için üretilmiş olan Stuxnet, ağ üzerinden kendini çoğaltmış ve birçok bilgisayara entegre olmuştur. 2011 yılında ise, Malezya'da hükümetin bazı web sayfalarına saldırılar olmuştur. Verilen siber savaş örneklerinden görüldüğü gibi siber savaşlar ile ülkeler oldukça zor durumlara düşürülebilmektedir. Siber savaşları gerçekleştirebilmek için siber silahlar kullanılmakta, bu silahlar kapsamlı ama düşük potansiyelli araçlardan özel ama yüksek potansiyelli silahlara kadar geniş bir yelpazeye yayılmaktadır [5, 14-18].

10.5. Siber Silah

Bilişim çağı ile birlikte yeni nesil bir silah kategorisi ortaya çıkmıştır: Siber silahlar. Siber silah kavramını daha net açıklayabilmek için öncelikle silah nedir genel hatlarıyla tanımlamak iyi olacaktır. Silah, yapılara, sistemlere veya canlılara fiziksel, işlevsel veya zihinsel zarar vermek veya tehdit etmek amacıyla kullanılan ya da kullanılmak üzere tasarlanmış bir araç olarak tanımlanabilmektedir. Günümüzde hedefe zarar verebilmek amacıyla, askeri alanda bomba, tüfek, füze gibi fiziksel silahların kullanımı devam etmektedir. Ancak, düşmanlar artık sadece fiziksel silahlarla yetinmemekte siber silahlarla internet üzerinden de ciddi şekilde saldırılar düzenlemektedirler. Siber silah, askeri savunma sistemlerinden finansal sistemlere kadar ülkelerin Tablo 10.2'de örneklenmiş kritik altyapılarını bozmaya yönelik veya hedef sistem üzerinde izleme, bilgi toplama yapabilecek veya sistemi çalışamaz hale getirebilecek herhangi bir yöntem, araç veya geliştirilen bir yazılım, virüs veya izinsiz girişler olarak tanımlanabilmektedir [13, 14, 19].

Son zamanlarda hemen hemen bütün devletler, şirketler, bireyler çağdaşlaşmanın etkisiyle bilgisayar sistemlerine bağımlı hale gelmiş durumdadırlar. Bilgisayar sistemlerine bu kadar bağımlı yaşamamız, doğal olarak bu sistemleri hedef haline getirmekte, saldırılar için çekici duruma düşürmektedir. Siber saldırganlar, hedef ülkelerin bilgisayar sistemlerine kilometrelerce uzaklıklardan rahatlıkla erişebilmekte ve zararlar verebilmektedirler. Ülkelerin sa-

vunma sanayileri de dâhil olmak üzere neredeyse tüm altyapılarının bilgisayar teknolojilerine bağlı olduğu düşünülürse, her ülkenin kendi bilgisayar sistemlerini sürekli kontrol altında tutması kendi güvenlikleri açısından oldukça önemlidir. Çünkü sınırları oldukça geniş ve değişken olan internet ortamında gerçekleştirilen bir saldırının kaynağının tespit edilmesi çok zor olmakta hatta bazen tespit edilebilmesi mümkün bile olmamaktadır. Siber savaşların hangi tür yazılımlarla ya da donanımlarla gerçekleştirilebileceği konusunda, hangi zararlı bilişim unsurlarının siber saldırı silahı olarak nitelendirilebileceği hakkında literatürde ortak bir karar bulunmamaktadır.

Tablo 10.2. Ülkelerdeki Kritik Altyapılar [20]

Bankacılık ve Finans
Kamu İdaresi
Bilgi ve İletişim Teknolojileri
Acil Durum / Kurtarma Hizmetleri
Enerji / Elektrik,
Sağlık Hizmetleri
Gıda/Tarım
Taşımacılık/Lojistik/Dağıtım
Su

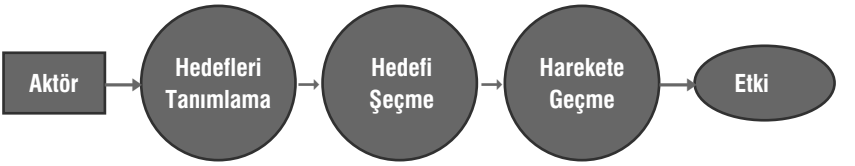
Siber silahların amaçlarının zarar vermek olduğu göz önüne alınırsa, bilgisayar sistemlerine ve ağlarına zarar verebilen sıradan ve basit bir DoS/DDoS saldırısı, Truva atları (trojen), solucanlar, virüsler, mantık bombaları ve benzeri zararlı yazılımlar birer siber silah olarak kabul edilebilmektedir. Virüsler bilgisayarın düzgün çalışmasını engelleyen ve bilgisayar içindeki kişisel bilgiler için tehdit oluşturan zararlı yazılımlardır. Virüslerin yayılabilmeleri kullanıcıların kendilerini bir şekilde diğer kullanıcılara göndermesi ile gerçekleşmektedir. Virüsler CD, DVD, USB bellek veya ağ yolu ile yayılabilmektedirler. Solucanlar ise, ana bilgisayara saldıran ve ağ üzerinden yayılan zararlı kodlar içeren programlardır. Genellikle web siteleri, ağ üzerinde paylaşılan dosyalar ve e-posta ile gönderilen ekler aracılığıyla yayılmaktadırlar. Solucanlar bir bilgisayara bulaştıktan sonra, kullanıcının yardımına ihtiyaç duymadan başka

kaynaklara ulaşarak kendilerini hızla çoğaltabilmektedirler. Örneğin, 1998 yılında ortaya çıkan CIH virüsü, Çernobil faciasının yaşandığı gün aktifleşmişti. Bu virüs sabit diskleri gereksiz kodlarla doldurarak devre dışı bırakıyor ve BIOS'lara zarar veriyordu. 2003 yılında kendini gösteren SQL Slammer solucanı ise kendisini rastgele bir IP üzerinden yolluyor, o IP'yi kullanan bilgisayarda SQL Server varsa bağlantısını kesiyordu. Görüldüğü gibi solucan veya virüslerle gerçekleştirilen saldırıların yarattığı mağduriyetler küçümsenecek boyutta değildir. Truva atı casus yazılımı, kullanıcılara kendisini yararlı bir program olarak göstererek sistemlere yüklenmelerini sağlamakta ve kullanıcının şifreleri de dâhil kişisel bilgilerine ulaşabilmektedir. Truva atı ilk bulaşmadan sonra hafızaya yerleşmekte ve sistem açıkları yardımı ile saldırganın isteklerini yerine getirmektedir. Örneğin, Loapi isimli Truva atı telefonunuza bulaştığında hayır cevabının kabul edilmediği bir istekle yönetici haklarını ele geçirmektedir. Yetkileri ele geçirdikten sonra, istenmeyen reklamlar gösterme ve paralı servislere abonelikler yapmaktan, başkaları adına kripto madencilik yapmaya kadar türlü işlemler yapabilmektedir. Bu işlemleri yaparken işlemci kullanımını %100'e çıkardığından, telefonlar bir süre sonra fazla ısınarak yanmaktadır. Siber silah olarak kabul edilebilecek bir diğer kötücül yazılım olan mantık bombaları ise, bir programın içerisine zararlı bir kod parçacığı yerleştirerek hedef sistemdeki tüm bilgilerin yok edilmesini sağlamaktadır. 1982 yılında mantık bombası ile Rusya'nın boru hatlarındaki akışı kontrol eden yazılıma müdahale edilmiş ve botu hattı patlatılmıştır. En yaygın siber silahlardan olan DDoS saldırıları ise, hedef sistemleri durdurarak maddi kayıplara sebep olmaktadır. Kritik altyapılara yapılan bir saldırı olmamasına karşın, sistemlerin bir kısmını hizmet dışı bırakabiliyor olması küçümsenecek bir etki değildir. Örneğin 2009 yılında gerçekleştirilen bir DDoS saldırısı ile Twitter saatlerce kapalı kalmıştır. Benzer şekilde 2012 yılında, THY'nin çevrimiçi uçuşlar sayfasına yapılan DDoS saldırıları yüzünden uçuşlarda aksamalar meydana gelmiştir [1, 13, 16, 21, 22].

Bahsedilen virüs, solucan, DDoS gibi siber silahların dışında, gelişmiş yapıya sahip, kritik altyapıları hedef alan, arkasında büyük desteklerin olduğu bilinen siber silahlar bulunmaktadır. Bu güçlü siber silahlara geçmeden önce siber silahların kavramsal tasarım modelinden ve mimarisinden kısaca bahsetmek iyi olacaktır.

10.5.1. Siber Silahların Kavramsal Tasarım Modeli

Bu bölümde, siber silahların kullanım durumlarını temsil eden kavramsal tasarım modelinden bahsedilecektir. Şekil 10.1'de verilen bu modelin her bir parçası ayrı ayrı ele alınarak ayrıntılı olarak incelenecektir.



Şekil 10.1. Siber Silahların Kullanım Durumunun Kavramsal Tasarım Modeli

Siber silahların kullanımına dayanan kavramsal tasarım modelinin parçalarını inceleyelim [23, 24]:

Aktör: Aktör, askeri hedeflere ulaşma amacına sahip siber operasyonları veya aktiviteleri yürütmeden sorumludur. Siber uzayın hızlı bir şekilde genişlemesi, kötü niyetli aktörlere ortam hazırlamaktadır. Dünyanın herhangi bir bölgesindeki bir aktör, verileri yok etmek, bozmak veya kritik sistemlere zarar vermek için binlerce kilometre uzaktaki bir ağa saldırabilmektedir. Siber silahların amaçlarına ulaşabilmesi için aktörler tarafından siber savaş içerisinde kullanılmaları gerekmektedir. Bu aktörler üç bölümde gruplandırılmış ve aşağıda açıklanmıştır [23-26].

10.5.1.1. Devlet Aktörleri

Devlet aktörleri, karmaşık düzeydeki siber silahları yetkilendirmek için güç, bilgi ve kaynaklara sahip devletler, hükümetler ve kurumlardır. Bu aktörler, milli çıkarlar için finanse edilmekte ve özel seçilmiş hedefe yönelik çalışmaktadır. Genellikle ekonomik, politik, teknik ve askeri motivasyonlara sahiptirler. Bu aktörler tarafından düzenlenen bir süreçte; birçok prosedür tasarlanmalı, takip edilmeli ve uygulanmalıdır. Bu da, sürecin beklenenden daha fazla zaman almasına sebep olabilmektedir. Devlet aktörleri ve aşağıda açıklanacak olan devlet dışı aktörler arasındaki fark, istihbarat, personel, ekipman gibi kaynakların kullanılabilirliğinde ve siber silahların uygulanması için kullanılan kalite, yenilikçilik ve akıllı yöntemlerde görülebilmektedir. Siber silahların büyük kısmı devlet aktörleri

tarafından üretilmesine rağmen, devlet dışı aktörler tarafından da yoğun şekilde üretim çalışmaları yapılmaktadır.

10.5.1.2. Devlet Dışı Aktörler

Devlet dışı aktörler, herhangi bir devlet aktörü ile ilişki kurmadan, siber silahları kendi başlarına organize etmeye, uygulamaya ve kullanmaya karar veren devlet dışı kurumlar, kuruluşlar, gruplar ve örgütlerdir. Bunların, kişisel, ekonomik, ideolojik veya etik gibi motivasyonları olabilmektedir. Devlet aktörleri tarafından düzenlenen bir süreçte birçok prosedür olduğundan, sürecin zaman aldığından bahsetmiştik. Devlet dışı aktörlerde ise bu süreç, karşılaştırmalı olarak daha az zaman almakta, süreç daha esnek ve daha dinamik olabilmektedir. Siber silahlar, konvansiyonel silahlar ile karşılaştırıldıklarında daha az paraya ve zamana ihtiyaç duymaktadırlar. Bu sebeple siber silahlar, devlet dışı aktörler tarafından yaygın şekilde kullanılmaktadır.

10.5.1.3. Karma Aktörler

Karma aktörler, devlet ve devlet dışı aktörlerin bir kombinasyonu olarak ifade edilmektedir. Bu kombinasyon, devlet dışı bir aktör tarafından desteklenen devlet aktörü veya devlet aktörü tarafından desteklenen devlet dışı bir aktör şeklinde olabilmektedir.

Amaçları Tanımlama: Amaçlar, aktörlerin ulaşmak istedikleri hedefler olarak tanımlanmaktadır. Amaçlarına ulaşabilmeleri için doğru hedefleri tanımlayıp seçerek harekete geçmeleri gerekmektedir.

Hedefi Seçme: Hedef, rakip üzerinde avantaj elde etmek için kullanılabilen varlık, nesne veya kişidir. Hedeflerin seçilmesi ve önceliklendirilmesi ile ilgili süreçler hedef belirleme süreci olarak isimlendirilmektedir.

Harekete Geçme: Bir aktör amaçlarını ve hedeflerini tanımlayıp planladıktan sonra bir siber silah kullanacaktır. Bu, bir dizi farklı etki türüne, bir operasyonun veya faaliyetin etkisine neden olacaktır. Siber silahlar bir hedef üzerinde belli bir amaç için kullanıldıklarında, aynı hedefte tekrar başarılı olma ihtimalleri düşüktür, çünkü saldırıya uğrayan taraf o silaha karşı güvenlik önlemleri alarak sa-

vunma mekanizmaları geliştirecektir. Bu sebeple özel bir amaç ve hedef için üretilen siber silahların tek kullanımlık olduğu söylenebilir.

Etki: Etki, bir eylemin veya başka bir etkenin fiziksel veya fiziksel olmayan sonucudur. Fiziksel etkiler somut nesneleri hedef aldıkları için oldukça önemlidir. Verilerin bütünlüğünü ve kullanılabilirliğini ihlal eden fiziksel olmayan etkiler, fiziksel hasar oluşturmaya çalışmaktan daha ucuzdur [27]. Siber silah kullanımının etkileri veya etki kategorileri aşağıdaki gibi tanımlanabilmektedir:

- *İstenen Etki*: Bu etki kategorisi, görevi yerine getirerek istenen nihai duruma katkıda bulunacak, istenen veya hedeflenen sonuçları tanımlamaktadır.
- *İstenmeyen Etki*: Bu etki kategorisi, istenen nihai duruma ulaşmayı olumsuz olarak etkileyecek istenmeyen sonuçları tanımlamaktadır.

Beklenti boyutu dikkate alındığında, istenen ve istenmeyen etki için geçerli kategoriler aşağıdaki gibi tanımlanabilmektedir:

- *Beklenen Etki*: Bu etki kategorisi, başlangıçta istense ya da istenmese bile beklenen sonuçları tanımlamaktadır.
- *Beklenmeyen Etki*: Bu etki kategorisi, sosyal, ekonomik, politik veya benzer konularla ilgili birçok sonuç doğurabilecek beklenmedik sonuçları tanımlamaktadır.

Siber silahların kullanım içeriklerine ait parçalar bu bölümde incelenmiştir. Bu parçaları tanımlayabilmek ve izleyebilmek için analiz edilmesi gereken yaşam döngüleri bulunmaktadır. Bu yaşam döngüleri bir sonraki bölümde ele alınacaktır.

10.5.2. Siber Silahların Yaşam Döngüsü

Saldırganların, siber silahlarla saldırılarını gerçekleştirebilmeleri için siber silahların yaşam döngüsünü oluşturan aşamaları tamamlamaları gerekmektedir. Siber silahların yaşam döngüsü incelendiğinde, siber silahlara ait tasarım mimarisinin, füzelerin temel unsurlarını barındırdığı görülmektedir. Füzeler; teslimat aracı olarak roket motoru, hedefe nasıl ulaşacağını belirleyebilmek için bir navigasyon sistemi, zarar veren bileşen olarak da bir yük içermektedir. Bu unsurlar incelendiğinde, siber silahların da aynı unsurları

içerdiği açıkça görülmektedir. Örneğin, siber silahları hedeflerine ulaştırmak için kötü amaçlı kod içeren e-postalar, zararlı bağlantılar barındıran web siteleri, sahte donanım ve yazılımlar, teslimat veya dağıtım aracı olarak kullanılmaktadır. Sistem açıklıkları, yazılım ve bilgisayar sistemlerindeki güvenlik açıklıkları veya diğer güvenlik riskleri; bir navigasyon sisteminin bir füzeye rehberlik etmesi gibi, kötü amaçlı yüklerin hedef noktaya ulaşmasını sağlamaktadır. Bir füzeye ait yük bazen bir çeşit patlayıcı olabilirken, siber silah için yük bilgi kopyalayan, değiştiren, yetkisiz kullanıma izin veren zararlı kodlar olabilmektedir. Bu bölümde siber silahların mimari tasarımını içeren yaşam döngülerinden ayrıntılı olarak bahsedilecek ve bu yaşam döngüsü on aşamada incelenecektir [23, 28-34]:

Proje Tanımı: Bu aşamada siber silah kavramı hem stratejik hem de yönetimsel açıdan tanımlanmakta, böylece siber silahın mimarisi oluşturulmuş ve ana işlevselliği tanımlanmış olmaktadır. Bu aşamada siber silahın ne yapması gerektiği açıkça belirlenmektedir.

Keşif: Bu aşamada, saldırgan hedef üzerinde araştırmalar yürütmekte ve bilgi toplamaktadır. Keşif kelimesi askeri kelime dağarcığından gelmekte, bir hedef bölge üzerinde stratejik gözlemler yapma sürecini tanımlamaktadır. Hırsızlar gibi siber suçlular da saldırılarını keşifler yaparak dikkatle planlamaktadır. Faydalı veri ve bilgi toplayarak yararlanılabilecek mevcut güvenlik açıklıklarını veya hizmetlerini bulabilmek için hedefle ilgili bir araştırma yapılmaktadır [32, 35-37]. Güvenlik açıklıkları, güvenlik sorununa neden olan yazılım veya donanım hataları olarak tanımlanmaktadır. Bu güvenlik açıklıklarından ve bu açıklıklar kullanılarak yapılan saldırılardan birkaç örnekle kısaca bahsedelim [38, 39]:

- *Sıfırıncı Gün (Zero Day)*: Daha önceden bilinmeyen ancak siber saldırılar için zafiyet oluşturulabilecek, yazılım veya donanıma ait tespit edilememiş güvenlik açığıdır. Bu açıklıklar farkedilip giderilene kadar birçok saldırı yapılabilmektedir.
- *Meltdown*: Speculative execution özelliğini kullanarak masaüstü ve dizüstü bilgisayarlar ile bulut tabanlı sunucuları etkileyebilen donanımsal bir güvenlik açığını kullanmaktadır. Meltdown, kullanıcı uygulamaları ile işletim sistemleri arasındaki temel izolasyonu kırmakta ve bellekte ulaşılmaması gereken bilgilere erişim sağlamaktadır [40, 41].

- *Spectre*: Meltdown'a benzer şekilde Speculative execution özelliği yardımı ile ARM, AMD, Intel işlemcilerini etkileyen donanımsal bir güvenlik açığını kullanmaktadır. Uygulamaların bellekte keyfi yerlere erişmelerine ve uygulamalardan bilgi sızdırılmasına sebep olmaktadır [41, 42].
- *Rowhammer*: DRAM işlemcilerde, bir dizi belleğe arka arkaya erişmenin yakınlardaki satırlarda bit değişikliklerine sebep olabileceği bir zafiyetten yararlanmaktadır [43, 44].

Burada kısaca örneklenenler gibi yazılımsal ve donanımsal birçok güvenlik açığı bulunmaktadır. Keşif aşamasında da amaç, saldırı için seçilecek sistem ve açıklıklar hakkında mümkün olduğunca fazla bilgi sahibi olmaya çalışmaktır. Toplanan bu bilgiler, siber silahların yaşam döngüsünün sonraki aşamalarında kullanılmaktadır [32, 35-37]. Keşif pasif ya da aktif olarak iki bölümde ele alınmaktadır [23, 35, 45]:

- *Pasif Keşif*: Pasif keşifte, hedef sistemle etkileşime girilmeden, saldırgan, sosyal medya veya kimlik avı gibi yöntemlerle bilgi toplamaktadır.
- *Aktif Keşif*: Saldırgan, kuruluşun kaynakları ile doğrudan etkileşime girerek bilgi toplamaktadır. Bu bilgiler, uygulamanın mimarisi, port bilgileri, kullandığı teknolojiler veya kullanıcı verileri gibi çeşitli bilgiler olabilmektedir.

Keşif aşaması ile saldırganın hedefe uygun silah tipi ve olası teslimat yöntemlerine karar vermesini sağlayacak potansiyel hedefler hakkında bilgi toplanmakta, bu bilgiler yaşam döngüsünün ileriki aşamalarında siber silahın geliştirilmesinde kullanılmaktadır. Siber silahların yaşam döngüsünü bu aşamada kırabilmek için sosyal mühendislik kullanımlarının önlenmesi ve URL filtreleme yolu ile bilinen kötü amaçlı URL'lerinin engellenmesi gibi önlemler gerekmektedir [29].

Tasarım: Bu aşamada keşif sırasında toplanan bilgiler kullanılarak, siber silahın gereksinimlere yanıt verecek temel yapısı oluşturulmaktadır. Burada siber silahın her bileşeni için ayrıntılı şekilde özellikler, görevler tanımlanmakta, geliştirme ekibinin projeyi uygulamasına yardımcı olacak diyagramlar, modeller kullanılarak siber silahın tasarımı yapılmaktadır.

Geliştirme: Bu aşamada, geliştirme ekibi çeşitli programlama dillerini kullanarak siber silahın tasarımına uygun olarak yazılımını geliştirmektedir.

Test: Bu aşamada, siber silahın kullanılacağı gerçek ortama yakın bir test ortamı hazırlanmakta ve saldırı karşısında siber silahın çalışması simüle edilmektedir. Siber silahın tüm bileşenleri için hataları ve hataları ile birlikte çalışabilirliği kontrol edilmektedir. İstenen hedeflere ulaşılıp ulaşılmadığını görmek için test prosedürlerinin tanımlanması ve uygulanması oldukça önemlidir.

Doğrulama: Bu aşamada test aşamasında elde edilen sonuçlar, proje tanımında ve tasarımında tanımlanan hedefler ve işlevselliklerle karşılaştırılmaktadır. Bu karşılaştırmanın sonucu olumlu olursa, siber silah hedef sisteme izinsiz girmeye hazır duruma gelmiş demektir. Karşılaştırma sonucunun olumsuz olması durumunda ise tasarım, geliştirme ve test aşamalarına geri dönülerek bu aşamalar tekrarlanmaktadır.

İzinsiz Giriş ve Kontrol: Bu aşama uzaktan yürütülen siber silahların önemli bir parçasıdır ve burada iki süreç söz konusudur. Bunlardan ilki, siber silahın hedef sisteme girdiği anı kesin olarak göstermektir. İkincisi ise, sistemi izlemek ve saldırıyı başlatmak için doğru anın ne zaman olacağına karar verebilmek için hedef sistemin kontrolünü ele geçirmektir [36].

Saldırı: Bu aşama yaşam döngüsünün en kritik aşamasıdır. Bu aşamada, siber silahın en önemli parçası, hedefi yerine getirmeye devam edecek olan yükler, harekete geçirilerek saldırı başlatılmaktadır. Yük, kötü amaçlı yazılımın temel içeriği olarak ifade edilmektedir. Bir yükün teslimi ve uygulanması kötü amaçlı yazılımın hedefidir. Basit kötü amaçlı bir solucanın yükü ile Stuxnet'in güçlü hasara sebep olan yükü kıyaslandığında, yüklerin karmaşıklığının çeşitlilik gösterdiği görülmektedir [27, 36].

Bakım: Bu aşamada, istenen etkilerin elde edildiğinden emin olmak için siber silahın hareketi izlenmektedir. Eğer plana göre olmayan şeyler varsa, sorunu çözmek ve saldırıya devam etmek için tedbirler alınacak, yazılımın iyileştirilmesi ve yeni işlevlerin eklenmesi yapılacak veya test aşamasına geri dönülecektir.

Dışarı Sızma: Bu aşamada, siber silahın yaşam döngüsü sona ermekte ve hedef sistemden çıkarılmaktadır.

Siber silahların kullanım durumlarını temsil eden kavramsal tasarım modelinden sonra siber silahların yaşam döngüsü de ayrıntılı olarak açıklanmıştır. Siber silahlar ayrıntılı olarak açıklandığına göre, büyük hasarlara sebep olmuş siber silahların örneklenmesi iyi olacaktır.

10.5.3. Yüksek Etkili Siber Silahlar

Gelişmiş yapıya sahip, kritik altyapıları hedef alan, iyi şekilde düzenlenip organize edilmiş, arkasında devletlerin veya büyük desteklerin olduğu bilinen, büyük hasarlara sebep olmuş ve bugünün dünyasında gerçek anlamda siber güvenliği tehdit eden güçlü siber silahların başında APT'ler gelmektedir. Bu saldırılar son dönemde çok etkili ve popüler saldırılar haline gelmiştir. Bu saldırılar, bu kitabın 11. Bölümünde detaylı olarak açıklanmış olsa da burada konunun daha iyi anlaşılması için aşağıda bazı örnekler verilmiştir.

- Night Dragon:

Night Dragon olarak etiketlenen saldırılar, 2009 Kasım ayından itibaren küresel petrol ve gaz şirketlerine karşı koordine edilmiştir. Gizli ve hedefe yönelik olarak Windows işletim sistemi açıklıklarını kullanarak bilgisayarlarda erişim hakkı elde etmişlerdir. Elde edilen erişimler ile petrol ve gaz saha üretim sistemleri ile ilgili ihale ve finansal bilgileri ele geçirmişlerdir [16, 46, 47].

- Stuxnet:

Haziran 2010'da Beyaz Rusya'daki VirusBlokAda ismindeki bir bilişim firması tarafından tespit edilmiştir. Stuxnet, İran'ın Natanz nükleer santrallerine zarar vermek amacıyla oluşturulmuştur. Böylece, tarihte ilk kez bir devletin kritik altyapısının bir kısmını imha etmeyi amaçlayan hedefe yönelik bir siber saldırı görülmüş olmuştur. Stuxnet, çeşitli mekanizma ve işlevselliklere sahip geniş ve karmaşık bir solucan parçasıdır. Stuxnet, çıkarılabilir sürücüler ile kendini çoğaltabilme, güncelleyebilme, bir LAN ortamında yayılabilme sonra da uzak sistemlerde çalıştırılabilme özelliklerine sahiptir. Bir USB bellek ile Natanz tesislerindeki bilgisayarlara bulaştırılmış ve kendini kopyalayarak çoğaltmıştır. Stuxnet zararlı yazılımı, PLC

(Programmable Logic Controllers) kontrol devrelerini ve gerçek zamanlı veri toplama, kontrol ve izleme yapan SCADA (Supervisory Control and Data Acquisition) sistemlerini etkiyerek hatalı çalışmalarına yol açmıştır. Nükleer santraldeki uranyum zenginleştirmede kullanılan çok sayıda santrifüjün kontrolünü yapan PLC kontrol devrelerini ele geçirmiş ve santrifüjlerin dönme hızlarını değiştirerek arızalanmalarına ve ömürlerinin azalmasına sebep olmuştur. Yazılım ortadaki adam saldırısı (man-in-the-middle attack) olarak gerçekleştirilmiş ve sabotajın algılanmasını önleyerek harici denetleyicileri yanlış verilerle besleyerek fark edilmesini önlemiştir. Bu yazılım ile İran'ın uranyum zenginleştirme programına ciddi darbe vurulmuş, İran'ın nükleer çalışmalarını neredeyse iki yıl kadar geriye götürmüştür [16, 22, 48-54].

- Duqu:

Duqu, Stuxnet'in tespit edilmesinden yaklaşık bir yıl sonra Ekim 2011'de Budapeşte'deki CrySyS laboratuvarında keşfedilmiştir. Yazılım çalınan verileri "DQ" ile başlayan dosya adlarında depoladığı için bu şekilde isimlendirilmiştir. Stuxnet ile çarpıcı benzerliklere sahip olduğu tespit edilmiş ve benzerlikleri dikkate alındığında Duqu'nun, Stuxnet'i yapan saldırganlar tarafından gerçekleştirildiği tahmin edilmiştir. Hedefinde İran, Sudan, Fransa ve Macaristan'ın bulunduğu Duqu'nun Stuxnet'ten farklı bir hedefi olduğu belirlenmiştir. Duqu fiziksel bir hasara neden olmayı değil, bilgi toplamak için siber casusluk yapmayı hedeflemektedir. Yazılım, MS Office Word programındaki True Type font sıfırıncı gün açığından faydalanarak yayılmıştır. Kendi kendini çoğaltma yeteneği olmayan Duqu, ağ paylaşımları yoluyla çoğaltılabilmiştir. Başarılı bir bulaşma gerçekleştikten sonra, saldırganlar şifreleri çalmak, ekran görüntülerini kaydetmek ve diğer hassas bilgi türlerini çalmak için kullanılabilecek bir keylogger da dâhil olmak üzere ek çalıştırılabilir dosyalarını indirmişlerdir. Duqu yazılımı 30 gün sonra bulaştığı makineden kendisini silmiştir, ancak yapılan incelemelerde saldırganların isterlerse bu süreyi uzatabilecekleri tespit edilmiştir. Duqu'nun hedefleri hakkında çok fazla bilgi olmasa da, gelecekteki saldırılara hazırlanmak için bilgi topladığına inanılmaktadır [16, 20, 48, 49, 52, 54, 55].

- Flame:

Flame, 2012 yılı Mayıs ayında tespit edilmiş ve Ortadoğu ülkelerini hedef almıştır. Flame, Stuxnet ve Duqu'dan farklı bir platform üzerine kurulmuş bir bilgi toplama yazılımıdır. Başka tür saldırılar araştırılırken tesadüfen tespit edilmiş olan yazılımın, yaklaşık olarak 5-8 yıldan beri aktif olduğu tahmin edilmektedir. Stuxnet ve Duqu ile kod yapısı ve fonksiyonlarında çok fazla olmasa da benzerlikler tespit edildiğinden, Flame'i gerçekleştirenlerin, Stuxnet ve Duqu'yu gerçekleştirenler ile işbirliği içinde oldukları tahmin edilmektedir. Yazıcı kuyruğu ve Windows Shell şeklindeki iki tane sıfırıncı gün açığını kullanan Flame yazılımı, Ortadoğu ülkeleri başta olmak üzere Windows tabanlı sistemlere saldırarak bilgi sızdırmayı hedeflemiştir. Flame, 20 MB'lık boyutu ve içerdiği yirmi modül sebebiyle, en büyük boyutlu kötü amaçlı yazılımlardan bir tanesidir. Yazılımın boyutunun büyük olması, yazılımın yüklenme ve indirilme sırasında uzun zaman alması ve yayılmasının zorlaşması gibi sebepler yüzünden dezavantaj oluşturmaktadır. Flame'in bu dezavantajlara rağmen büyük boyutlu olması kontrollü yayılma ve belirli alanda (Ortadoğu) daha fazla bulaşma planlandığını işaret etmektedir [16, 48, 52, 54].

- Kırmızı Ekim (Red October):

2012 Ekim ayında güvenlik şirketi Kaspersky Labs tarafından duyurulan Kırmızı Ekim yazılımı, uluslararası diplomatik ve resmi kurumlardan gizli belgeleri çalmak amacıyla oluşturulmuştur. Kaspersky firmasının iddiasına göre, saldırganların temel hedefi sonraki saldırılarda kullanmak üzere istihbarat toplamaktır. Saldırı, kötü amaçlı yazılımın gömülü olduğu MS Office ve Excel dosyalarının ekli olduğu spear phishing e-postaları yardımı ile gerçekleştirilmiştir. Kötü amaçlı yazılım Word, Excel ve pdf görüntüleyicideki bilinen güvenlik açıklarından yararlanmak üzere tasarlanmıştır. Zararlı yazılım bulaştıktan sonra, ana bileşeninin kurulumunu başlatarak C&C (Command and Control) sunucuları ile daha fazla iletişim kurmaya başlamıştır. Yazılım geniş bir yelpazedeki görevlerini yerine getirebilmek için özel olarak oluşturulmuş modüllerini indirip çalıştırmaktadır. Örneğin bu modüllerden birisi Nokia cep telefonları ve Iphone'lardan bilgi çalma üzerine ayarlanmıştır. Kır-

mızı Ekim yazılımı, minimalist bir mimariye sahip olması ve şifreli modüllerini indirerek bellekte çalıştırması sayesinde başlarda kendini başarıyla gizlemeyi başarmıştır [16, 52, 54].

- Gauss:

Haziran 2012'de Kaspersky Labs tarafından keşfedilen Gauss, Flame platformuna dayanan ve Ortadoğu'yu hedef alan bir bilgi toplama yazılımıdır. Gauss yazılımı, Stuxnet, Duqu ve Flame'in akrabası olarak tanımlanabilmektedir. Lübnan'da 1600'den fazla bireysel bilgisayara, İsrail'de ise 500 civarında bilgisayara bulaşarak Duqu ve Flame'den daha yaygın hale gelmiştir. Modüllerinde kendini çoğaltma özelliği tespit edilemeyen Gauss yazılımı, Microsoft Windows işletim sisteminin Xp, Vista ve 7 sürümlerini hedeflemektedir. Sayısal yeteneklere sahip olan Gauss, bulaştığı sistemden mümkün olduğu kadar fazla bilgi toplamak için tasarlanmıştır. Özellikle bankacılık sistemlerinden, sosyal ağlardan ve e-posta hesaplarından bilgi çalmayı hedeflemektedir [48, 52].

- Siyah Enerji (Black Energy):

2015 yılında Ukrayna'da keşfedilmiş olan Siyah Enerji, Ivanı-Frankivsk bölgesindeki enerji santralini hedef almıştır. Uzmanlar, Siyah Enerji'nin pek çok şehrin birkaç saat enerjisiz kalmasına sebep olduğunu ve bilgisayarlar ile telefon hatlarını tahrip ettiğini belirtmişlerdir [23].

Yukarıda popüler örnekleri verilmiş olan güçlü ve hedef odaklı siber silahlar, hedeflerinin kritik altyapılarına saldırılar yapmakta ve hedeflerine maddi, manevi çok ciddi zararlar vermektedirler. İyi organize edilmiş, karmaşık yapıya sahip bu siber silahların ancak çok güçlü desteklerle ve alanında uzman ekipler tarafından geliştirilebileceği oldukça açıktır. Bu silahlarla gerçekleştirilen saldırılar karşısında, hedef ülkelerin çaresiz kaldıkları da oldukça açık şekilde görülmektedir.

10.6. Siber Silah Pazarı

Büyük bir katılımcı havuzuna sahip olan küresel siber silah piyasası, oldukça rekabetçi bir ortam sergilemektedir. BAE Systems, General Dynamics, AVG Technologies, Avast Software, Symantec Corporation, Kaspersky Lab, Cisco Systems, McAfee, Boeing, Lock-

heed Martin şirketi siber silahların temel tedarikçileri arasında sayılmaktadır. Siber silah pazarındaki bu aktörler, var olan ürünlerine gelişmiş teknolojileri dâhil edebilmek gibi sebeplerle yeniliklere odaklanmaktadırlar. Siber silah pazarında hem saldırı hem de savunma amaçlı siber silahlar bulunmaktadır. Zion Market Research tarafından yapılan araştırmada, savunma silahlarına olan talebin, saldırı silahlarına olan talebe oranla daha yüksek olduğu ifade edilmiştir. Siber suçlular tarafından saldırgan biçimde kullanılan siber silahlar sebebiyle kolluk kuvvetleri de savunma amaçlı siber silah kullanımına hız vermekte, bu da pazar talebini etkilemektedir. Hayati önem taşıyan özel ve resmi kuruluşlar, kritik altyapılarına yönelik siber saldırılar sebebiyle desteğe ihtiyaç duyduklarından, ilerleyen zamanlarda siber silah pazarının önemli bir büyümeye tanık olması beklenmektedir. Günümüzde, siber silah piyasasına Kuzey Amerika liderlik etmektedir ve bu liderliğin bir süre daha devam edeceği öngörülmektedir. Kuzey Amerikanın siber silah pazarındaki hakimiyetinin ana sebebi, siber silahların havacılık ve savunma sektörleri ile istihbarat birimlerinde yoğun olarak kullanılıyor olmasıdır. Pazar aktörlerinin büyük çoğunluğunun Kuzey Amerika'da bulunması da, bölgede siber silah pazarının büyümesini destekleyen önemli bir faktör olmuştur. 2022 yılındaki gelirinin yaklaşık 524 milyar dolarlara ulaşması beklenen küresel siber silah pazarı, Tablo 10.3'teki gibi sınıflandırılabilmektedir [56-58].

Tablo 10.3'ten de görülebileceği gibi, küresel siber silah pazarının bölümlenmesi türe, uygulamaya ve bölgeye göre yapılabilmektedir. Siber silahlar hem saldırı hem de savunma amacıyla kullanıldıklarından, silah pazarı bu iki türe göre ayrılabilmektedir. Siber silah pazarının bölümlenmesi ulusal savunma sistemleri, hava trafik kontrolü veya endüstriyel kontrol sistemi gibi uygulamalar temelinde de yapılabilmektedir. Siber silah pazarı coğrafi olarak ele alındığında ise, Kuzey Amerika, Avrupa, Asya Pasifik, Latin Amerika, Orta Doğu ve Afrika şeklinde gruplanabilmektedir. 2025 yılı sonunda bölgelerin pazar payı tahmini yapıldığında, Kuzey Amerikanın silah pazarındaki liderliğini koruması, en hızlı büyümenin de Asya Pasifik pazarında olması beklenmektedir. Türkiye'nin de siber alandaki gelişmelere ayak uydurabilmesi, milli güvenliğine katkı sağlamayabilmesi ve bu pazarda ön sıralarda yer alabilmesi için çalışmalarını hızlandırması gerekmektedir [56-58].

Tablo 10.3. Küresel Siber Silah Pazarı Sınıflandırması

Türe Göre	Uygulamaya Göre	Bölgeye Göre
• Savunma • Saldırı	• Ulusal Savunma Sistemi • Hava Trafik Kontrolü • Hastane • Otomatik Taşıma Sistemi • Endüstriyel Kontrol Sistemi • İletişim Ağı • Akıllı Güç Şebekesi • Diğerleri	• Kuzey Amerika • Avrupa *(İngiltere, Fransa Almanya)* • Asya Pasifik *(Çin, Japonya, Hindistan)* • Latin Amerika *(Brezilya)* • Orta Doğu ve Afrika

10.7. Siber Risklere Karşı Savunma

Aon Global Risk Consulting'in 2018 Siber Güvenlik Tahminleri Raporu'na göre büyük ölçekli siber saldırılar gerçekleşmeye devam etmekte ve bu saldırılara karşı koyabilmek için çeşitli önlemlerin alınması gerekmektedir. Dünya ortalamasının altında olan savunma bütçelerimizin doğru konumlandırılması ve kritik altyapılar için önceliklendirme yapılması büyük önem arz etmektedir. Siber tehditler konusunda önerilmiş bazı savunma stratejileri ile güçlü siber silahlarla gerçekleştirilmiş siber saldırılar önlenemese de, siber olayların bir kısmının engellenebileceği tahmin edilmektedir. Bu savunma stratejilerinden bir kısmı aşağıda verilmiştir [59].

Güvenilir Uygulamalar Listesi: ICS-CERT'e göre siber saldırıların bir kısmı güvenilir uygulamaların kullanılmaması sonucu oluşan zafiyetleri kullanmaktadır. Bu sebeple, güvenilir uygulamalar listesi, kötü niyetli yazılımların tespit edilmesi ve önlenmesinde önemli savunma stratejilerinden bir tanesidir.

Güncellemelerin ve Doğru Konfigürasyonların Yapılması: ICS-CERT'e göre güncellemeleri yapılmayan sistemler siber tehditlere açık hale gelmektedir. Bu sebeple güncellemelerin düzenli olarak yapılması tavsiye edilmektedir.

Saldırıya Maruz Kalınabilecek Alanların Azaltılması: Saldırıya maruz kalınabilecek internet ağı gibi alanların kullanılmayan port-

larının kapatılması veya dış ağlara erişim izinlerinin kontrol edilmesi önem arz etmektedir.

Savunulabilir Bir Ortam Kurulması: Sisteme girmeyi başaran saldırganların erişimlerini kısıtlayabilmek için ağları mantıklı şekilde bölümlere ayırmak önemli avantajlar sağlayacaktır.

Yetkilendirme Yönetiminin Uygulanması: Saldırganlar tarafından hesaplar çalındığında en az hasarla çıkabilmek için, kullanıcılara geniş yetkiler vermek yerine sadece ihtiyacı olan yetkiler verilerek kısıtlanmaları iyi olacaktır.

Güvenli Uzaktan Erişim Uygulamalarının Kullanılması: Açık olan tüm erişimlerin mümkün olabildiğince kısıtlanması veya ortadan kaldırılması da katkı sağlayacaktır.

İzleme ve Müdafaa Uygulamalarına Başvurulması: Sistemlerin siber tehditlere karşı korunması için sürekli gözlemler yapılarak önlemlerin alınması ve tepki verilmesi gerekmektedir.

Bahsedilen bu önlemler yüksek etkili silahlarla gerçekleştirilen siber saldırıları önlemek için etkili olamasa da siber güvenliğe katkı sağlayacaktır.

10.8. Siber Güvenlik Harcamaları

Yaşanan teknolojik gelişmeler neticesinde, siber savaş ve siber silah gibi siber tehditlerin hayatımızdaki yeri artmaktadır. Bu sebeple, ülkeler ulusal güvenlikleri için siber güvenlik harcamalarına da önem göstermektedir. Son 5 yıllık süreç incelendiğinde güvenlik harcamalarındaki artış açıkça görülmektedir. Gartner'ın analizlerine göre, güvenlik harcamaları 2013 yılında dünya genelinde 67,2 milyar dolar iken bu harcamalar son 5 yılda yüzde 29 artış göstermiştir. Bilim Sanayi ve Teknoloji Bakanı tarafından yapılan açıklamaya göre ülkemizin son 5 yılda yaptığı siber güvenlik harcamaları ise 340 milyon dolar civarındadır. 2019 yılında dünya genelindeki siber güvenlik harcamalarının 108 milyar dolara ulaşması, 2021 yılına kadar da 1 trilyon doları aşması beklenmektedir [59]. Ülkemizin kritik altyapılarını ve verilerini korumak, ülke güvenliğini ve siber güvenliği sağlamak için ciddi bütçeler ayrılarak planlı harcamalar yapılması oldukça önemlidir.

10.9. Değerlendirmeler

Bilgi ve iletişim teknolojilerinin ve özellikle de internetin hayatımızın ayrılmaz bileşeni olması siber güvenlik risklerini de beraberinde getirmiştir. Siber Güvenlik konusu özellikle 2008 yılından itibaren AB (Avrupa Birliği), OECD (Ekonomik İşbirliği ve Kalkınma Teşkilatı), NATO (Kuzey Atlantik İttifakı) gibi uluslararası kuruluşların ve tüm gelişmiş ülkelerin gündemine girmiştir. Türkiye siber güvenlik olaylarına karşı çalışmalarına hala devam etmektedir. Türkiye'de siber suçlarla mücadele, 2012 yılına kadar Bilgi Teknolojileri ve İletişim Kurumu tarafından sivil toplum kuruluşları ile birlikte yürütülmüştür. 20/10/2012 tarih, 28447 sayılı Resmi Gazetede yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonunu sağlamak görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir. Ülkemizde dağınık durumda olan siber güvenlik mevzuatı ele alınmalı ve tüm paydaşların katılımıyla ortak kabul edilen bir Siber Güvenlik Kanunu çıkartılmalıdır. Siber Güvenlik Stratejilerinin takibi ve etkin şekilde uygulanabilirliği kontrol edilmelidir. Tüm gelişmiş ülkelerin kendi siber güvenlik çalışmalarını yürütmeleri önemli olmasına rağmen, uluslararası güvenlik için bir birliktelik de oldukça gereklidir. NATO üyesi devletler de, Mayıs 2012'de gerçekleştirilmiş olan Chicago Zirvesi'ndeki bildirgede, "Siber güvenlik tehditlerini belirlemek ve ortak güvenliğimizi geliştirmek için somut işbirliğini arttırmak amacıyla ilgili ortak ülkelerle ve uluslararası kuruluşlarla beraber çalışmaya kararlıyız" cümlesi ile uluslararası işbirliğinin gerekliliğini ifade etmişlerdir [3, 4, 60].

Çok uzun bir geçmişe sahip olmayan siber savaşlar ve güçlü siber silahlar, günümüzde elektronik ortamda faaliyet gösteren tüm kurum ve kuruluşlar ve haliyle ülke içerisindeki tüm vatandaşlar için büyük bir tehlike arz etmektedir. Siber silahlar yardımı ile gerçekleştirilen saldırıların stratejik öneme sahip hedeflere yapıldığı ve çok ciddi zararlar verdiği gayet açık şekilde görülmektedir. Gün geçtikçe saldırıların sayısının ve kapsamının artacağı göz önünde bulundurulursa, kurum ve kuruluşların hızla gerekli önlemleri almaları

gerekmektedir. Özellikle ulusal kritik altyapılara sahip kurumların, hedefe odaklı siber silahlarla yapılan saldırıların zararlarının ne kadar yüksek olduğunu görmeleri sağlanmalıdır. 2011 yılında ABD Savunma Bakanlığı siber silahın tanımı ile ilgili uluslararası bir fikir birliği bulunmadığına işaret etmiştir. Siber silah için ortak bir fikir birliği sağlanmalıdır. Siber saldırılar, arkalarındaki güçlü destek ile son derece eğitimli kişiler tarafından gerçekleştirildikleri için, hedeflerine ulaşma konusunda sıkıntı yaşamamaktadırlar. Bu sebeple, bu saldırıların tespiti güç olsa da, ülke genelindeki elektronik faaliyetlerin olduğu kurum ve kuruluşlarda; ağ üzerinde trafiği izleme, analiz etme gibi çalışmalar yapılmalı böylece de herhangi bir olağan dışı durumda bunun tespit edilerek önlem alınabilmesi sağlanmaya çalışılmalıdır. Zararlı yazılımlar sıfırıncı gün hatalarından veya yazılımsal/donanımsal açıklıklardan yararlandıklarından, uzmanların bu açıkları takip ederek insanları çeşitli yollarla bilgilendirmeleri olumlu bir gelişme olacaktır. Tüm çalışanların ve kullanıcıların siber silahlar, siber savaşlar konularında bilinçlendirilmesi ve ülke genelinde farkındalık sağlanması oldukça önemlidir. Siber güvenlik alanında kendini geliştirmek isteyen personel, öğrenci ve araştırmacıların teşvik edilmesi ve böylece bu alandaki çalışmaların hız kazanarak dışa bağımlılığın azalması sağlanabilecektir. Bu alanlar için özel ve ciddi bütçeler ayrılarak, ihtiyaç duyan kurum veya kişilere destekler sağlanmalı, akademi, kamu ve özel sektörün bu alanlarda birlikte çalışmaları konusunda teşvikler yapılmalıdır. Milli ürünlerin olmadığı bir siber savaşı kazanmamız mümkün olmadığı için, nitelikli personellerin yerli fikirler, teknoloji tasarımları ve üretim konusunda teşvik edilmeleri gerekmektedir. Bu saldırıların tamamen engellenmesi her ne kadar mümkün olmasa da, zararları en aza indirmeye çalışmak ülke olarak hedefimiz olmalıdır.

Kaynaklar

[1] Aslay, F., *Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi*, International Journal of Multidisciplinary Studies and Innovative Technologies, 2017. 1: p. 24-28.

[2] Öpöz, S., *Siber Güvenlik*, T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, 2016.

[3] Akyazı, U., *Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler*, *6th International Information Security and Cryptology Conference*, 2013.

[4] Kasapoglu, C., *Cyber Warfare: Between the Future Military Reality and Today's Science-Fiction,* EDAM Cyber Policy Paper Series 2017/2, 2017.

[5] Alkan, M., *Siber Güvenlik ve Siber Savaşlar*, Bilgi Güvenliği Derneği, 2012.

[6] Ünver, M., Canbay, C., *Ulusal Ve Uluslararasi Boyutlarıyla Siber Güvenlik.* EMO- Elektrik Mühendisliği, 2010 (438): p. 94-103.

[7] Bodeau, D.J., Graubart, R., and Fabius-Greene, J., *Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels*, *IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust*, 2010.

[8] Yılmaz, S., Sağıroğlu, Ş., *Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri*, *6th International Information Security & Cryptology Conference*, 2013.

[9] Güdek, Ş., *20. Yüzyılı Aşırılaştıran ve Aşırılaşan Savaş Algısı-Pratiği*, BEU Akademik İzdüşüm/ Academic Projection 2017: p. 79-103.

[10] Dedemen, F., *Geleceğin Güvenlik Ortamının Şekillenmesinde Hibrit Savaş Modelinin Değerlendirilmesi,* Güvenlik Bilimleri Dergisi, 2016: p. 141-176.

[11] *2941 Sayılı Seferberlik Ve Savaş Hali Kanunu,* 4/11/1983: Resmi Gazete.

[12] Varlık, A.B., *Savaşı Tanımlamak: Terminolojik Bir Yaklaşım,* Avrasya Terim Dergisi, 2013: p. 114-129.

[13] Ege, B., *Siber Savaşlar Bilişimin Karanlık Yüzü,* Bilim ve Teknik Dergisi, 2012.

[14] Rid, T., McBurney, P., *Cyber-Weapons,* The RUSI Journal, 2012, **157**(1): p. 6-13.

[15] Yılmaz, S., Sağıroğlu, Ş., *Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi*, *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 2013, Ankara.

[16] Akın, M., Sağıroğlu, Ş., *Advanced Persistent Threats,* Türkiye Bilişim Vakfı Bilgisayar Bilimleri Ve Mühendisliği Dergisi, 2017, **10**(1): p. 1-10.

[17] Line, M.B., Tøndel, I.A., Jaatun, M.G., *Cyber Security Challenges in Smart Grids, 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2011, Manchester, p. 1-8, UK.

[18] Park, W.H., *A Study on Risk Analysis and Assessment of Damages to Cyber Attack, 2010 International Conference on Information Science and Applications*, 2010, Seoul, South Korea: IEEE.

[19] Yayla, M., *Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı*, Hacettepe HFD, 2014(4(2)): p. 181-200.

[20] Chien, E., Omurchu, L., Falliere, N., *W32.Duqu: The Precursor to the Next Stuxnet, 5th USENIX Workshop on Large Scale Exploits and Emergent Threats*, 2012.

[21] İstanbul Üniversitesi, *Siber Saldırı Türleri,* Bilişim'de Kariyer, (2): p. 11-14.

[22] Çelik, Ş., *Stuxnet Saldırısı Ve Abd'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme,* Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 2014, 15(1): p. 137-175.

[23] Maathuis, C., Pieters, W., Den Berg, J.V., *Cyber weapons: a profiling framework, 2016 International Conference on Cyber Conflict (CyCon U.S.)*, 2016, IEEE, p. 1-8.

[24] Mele, S., *Cyber-Weapons: Legal And Strategic Aspects, Observatory Infowarfare and Emerging Technologies*, Machiavelli Editions, Editor, 2013.

[25] US Department of Defense, *The Department of Defense Cyber Strategy*, April 2015.

[26] Güntay, V., *Transformation of Cyber Security into an Effect Tool, International Politics and International Actors,* Güvenlik Stratejileri, 2014(27).

[27] Herr, T., *PrEP: A Framework for Malware & Cyber Weapons,* The Journal of Information Warfare, 2014, Vol.13.

[28] Anonim, *How to Break The Cyber Attack Lifecycle,* https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle, (Son Erişim Tarihi: 05.12.2018).

[29] Palo Alto Networks: Reinventing Enterprise Operations and Defense, *Breaking the Cyber Attack Lifecycle,* 2015.

[30] Anonim, *Cyber Attack Lifecycle,* http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/, (Son Erişim Tarihi: 01.12.2018).

[31] Anonim, *Malware Lifecycle: Process of a Cyber Attack*. https://redsocks.eu/blog-2/malware-lifecycle-process-of-a-cyber-attack/, (Son Erişim Tarihi: 25.04.2018).

[32] Petersen, C., *The Threat Lifecycle Management Framework Protecting Insurers' Data And Reputation from Damaging Cyber-Attacks*, LogRhythm The Security Intelligence Company, 2017, Vol.9.

[33] Robinsona, M., Jones, K., Janicke, H., *Cyber warfare: Issues and challenges,* Journal of Computers and Security, 2015.

[34] Coleman, K.G. *Preparing for a Cyber Attack*, https://slideplayer.com/slide/3914644/, (Son Erişim Tarihi: 15.12.2018).

[35] Deloitte Touche Tohmatsu Limited, *7 Stages of Cyber Kill Chain Supplementary Reading*, 2017.

[36] Yadav, T., Mallari, R.A., *Technical Aspects of Cyber Kill Chain,* Cryptography and Security, 2016.

[37] Trend Micro, *Understanding Targeted Attacks: Six Components of Targeted Attacks*, 2015,

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/targeted-attacks-six-components, (Son Erişim Tarihi: 05.12.2018).

[38] Shah, S. *Cross Border Cyber Attacks: Impact on Digital Sovereignty*, *24th All India Forensics Sciences Conference*, 2018, Ahmedabad.

[39] Ünüver, C., *Vulnerability Market*, in *The Market for Cyber Weapons - NATO Cooperative Cyber Defence Centre of Excellence*, S. Ltd., Editor, 2014.

[40] Raytheon, *The Meltdown and Spectre Cyber Attacks,* White Paper, 2018.

[41] Koşaroğlu, A.İ., Yılmaz, D.E., *CPU Açıkları: Meltdown, Spectre*, *e-bergi*, 2018.

[42] The European Union Agency for Network and Information Security, *Meltdown and Spectre: Critical processor vulnerabilities*, 2018, https://www.enisa.europa.eu/publications/info-notes/meltdown-and-spectre-critical-processor-vulnerabilities, (Son Erişim Tarihi: 15.01.2019).

[43] Kim, Y., Daly, R., Kim, J., Fallin, C., Lee, J.H., Lee, D., Wilkerson, C., Lai, K., Mutlu, O., *RowHammer: Reliability Analysis and Security Implications,* 2016.

[44] Seaborn, M., Dullien, T., *Exploiting the Dram Rowhammer Bug to Gain Kernel Privileges,* 2015.

[45] Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, *Güvenli Yazılım Geliştirme Kılavuzu*, 2018.

[46] Command Five Pty Ltd, *Advanced Persistent Threats: A Decade in Review*, 2011.

[47] Miller, B., Dale, C.R., *A Survey of SCADA and Critical Infrastructure Incidents*, *Proceedings of the ACM Research in Information Technology*, 2012, Calgary, Alberta, Canada.

[48] Bencsáth, B., Pék, G., Buttyán, L., Félegyházi, M., *The Cousins of Stuxnet: Duqu, Flame, and Gauss,* Future Internet, 2012: p. 971-1003.

[49] Faisal, M., Ibrahim, M., *STUXNET, DUQU and Beyond,* International Journal of Science and Engineering Investigations, 2012, 1(2): p. 75-78.

[50] Güngör, U., Güney, O., *Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş,* Karadeniz Araştırmaları Dergisi, 2017: p. 131-146.

[51] Langner, R., *Stuxnet: Dissecting a Cyberwarfare Weapon,* IEEE Security & Privacy, 2011, 9(3): p. 49 - 51.

[52] Wangen, G., *The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism,* Information, 2015, 6: p. 183-211.

[53] Farwell, J.P., Rohozinski, R., *Stuxnet and the Future of Cyber War,* Survival Global Politics and Strategy, 2011.

[54] Virvilis, N., Gritzalis, D., *The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?, 2013 International Conference on Availability, Reliability and Security*, 2013, Regensburg, Germany: IEEE.

[55] Bencsáth, B., Pék, G., Buttyán, L., Félegyházi, M., *Duqu: Analysis, Detection, and Lessons Learned,* Proceedings of the ACM European Workshop on System Security (EuroSec'12), 2012.

[56] Zion Market Research, *Cyber Weapon Market To Report Impressive Growth, Revenue To Surge To US$ 524.27 Billion By 2022, Cyber Weapon Market*, 2018.

[57] Grand View Research, *Cyber Weapon Market Analysis, Market Size, Application Analysis, Regional Outlook, Competitive Strategies, and Forecasts, 2015 To 2022*.

[58] ReportBuyer, *Global Cyber Weapons Market Forecast 2017-2025*, 2017: London.

[59] Anonim, *Siber Saldırılara Karşı 7 Etkin Savunma*, 2018, https://www.btgunlugu.com/siber-saldirilar-a-karsi-7-etkin-savunma/, (Son Erişim Tarihi: 01.12.2018).

[60] *2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı.*

Siber Tehditlerde Son Nokta: İleri Düzey Kalıcı Tehditler

BÖLÜM 11

Murat AKIN - Prof. Dr. Şeref SAĞIROĞLU

SİBER TEHDİTLERDE SON NOKTA: İLERİ DÜZEY KALICI TEHDİTLER

Virüsler, solucanlar ve casus yazılımlar üzerinden yapılan saldırıların yanı sıra son on beş yıllık süreçte geliştirilen ve adına "gelişmiş sürekli/kalıcı tehditler" denilen, tamamen hedefe odaklı, iyi şekilde düzenlenmiş, organize olmuş ve en önemlisi arkasında büyük organizasyonlar, destekler veya devletler olduğu bilinen yeni bir saldırı türü ortaya çıkmıştır. Bu bölümde, ISC Turkey 2016'da sunduğumuz [1] ve TBV Bilgisayar Bilimleri ve Mühendisliği Dergisinde yayımlanan makalemizin [2] içeriği ile kapsamı genişletilmiş, güncellenmiş, yeni kısımlar eklenmiş ve yeni bir bakış açısıyla bu bölümde sunulmuştur. Bu bölümde, İleri Düzey Gelişmiş Tehditlerin (APT-Advanced Persistent Threats) genel yapısı ve karakteristik özellikleri sunulmuş, mevcut saldırılar incelenmiş ve sonuçta bu saldırılara/tehditlere karşı alınabilecek önlemler çok kapsamlı olmasa da özde sunulmuş ve bu riske karşı alınabilecek önlemler ile karşılaşılabilecek riskler konusunda değerlendirmelerde bulunulmuştur.

11.1. Giriş

Son yıllarda kurum ve kuruluşlara yapılan siber saldırıların sayısının giderek arttığı, daha karmaşıklaştığı, kapsamı ve boyutunun genişlediği, pek çok yenilikleri içerdiği, yeni modelleri, yapıları ve sistemleri içerisinde barındırdığı bilinmektedir. Bu değişim ve dönüşümlere bakıldığında siber korsanların/saldırganların;

- Organize olan tam donanımlı korsanlara dönüştükleri,
- Her türlü teknik ve teknolojileri, metot ve metodolojileri, araç ve yöntemleri, organizasyonları, altyapıları, geliştirme ortamlarını, kullandıkları,

- Deep web, Dark net vb. ortamları kullandıkları ve/veya faydalandıkları,
- Ekip, takım veya grup çalıştıkları,
- Hedeflerine odaklı oldukları,
- Kurumsal/Sektörel ağları hedefledikleri,
- Mobil, bulut ve sanallaştırma teknolojilerini içine alan saldırılar yaptıkları,
- BT altyapısında kullanılan modellerde değişiklikler, klasik güvenlik tedbirlerini devre dışı bırakma, sistemlerde arka kapılar oluşturma, sistemlere istenildiğinde kolay erişilebilir ortamlar hazırladıkları,
- Hükümetler, istihbarat servisleri tarafından sabotaj veya casusluk yapma amaçlı olarak görevlendirildikleri,
- Her türlü zafiyeti kullandıkları,
- Uzun vadeli ve hedefi iyi belirlenmiş, destekleyici olarak arkasında devlet veya büyük organizasyonların bulunduğu saldırıları gerçekleştirdikleri,
- APT olarak bilinen saldırıları planladıkları, hayata geçirdikleri, amaca odaklandıkları ve bunu uzun zaman olsa da yerine getirdikleri, bilinmektedir.

Ayrıca, bugünün dünyasında gerçek anlamda siber güvenlik ve savunma için yeni nesil çözümler, yaklaşımlar, teknolojiler kullanılmakta ve teknolojik sistemler için tehlikeler, saldırılar ve açıklıklar ise ciddi tehdit oluşturmaktadır. Dolayısıyla;

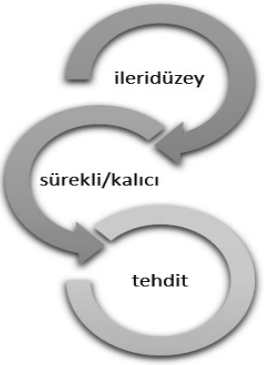
- Bu tehditleri anlamak, kapsamını bilmek, vereceği zararları öngörmek, sistemlerde oluşan tehditleri yakinen takip etmek ve gidermek, güncel saldırıları ve tehditleri bilmek, sistemi sürekli takip ve analiz etmek çok önemlidir.
- Sadece gerçek tehditleri fark ederek hedefli saldırı yöntemlerinin ve tekniklerinin daha geniş alanda nasıl ilişkili olduğunun görülmesi, kuruluşların gelecek yıllar içinde sahip oldukları bilgiler için koruyucu nitelikte bir siber kalkan olacağı bakış açısıyla çalışılmalıdır.

- Tehditleri anlamak, değerlendirmek ve karşı koymak için takım çalışması, ortak değerlendirme ve önceden hazırlık yapılmalıdır.
- Sistemlerin yakından izlenmesi, denetlenmesi, kontrol edilmesi, iyileştirilmesi, sıkılaştırılması ve karşılaşılabilecek risklerin öngörülüp giderilmesi gereklidir. Güncel politikalar çerçevesinde bu işlemler yapılmalıdır.
- Geliştirilen/kullanılan/kurulan her sistem, yazılım veya donanımla ilgili olarak mümkün olduğunca her türlü bilgi, klavuz, kaynak veya dokümandan alınabilecek en fazla bilgi elde edilmelidir.
- Kullanılan sistem, aygıt, yazılım veya yaklaşımlar test edilmeden kullanılmamalıdır.
- Standartları yüksek çözümler kullanılmalıdır.
- Belirlenen politikalara göre sızma testleri yapılmalı, sistemler sağlıklı, hijyenik ve korunaklı hale getirilmelidir.
- Mümkünse yerli ve milli çözümler geliştirilmeli ve geliştirilen çözümler, mutlaka uluslararası standartlara uygun hale getirilerek kullanılmalıdır.

11.2. İleri Düzey Sürekli / Kalıcı Tehditler

Yukarıda anlatılanlardan da açıkça görülebileceği gibi siber tehditler gittikçe gelişmekte ve değişmektedir. Son dönemde karşılaşılan ve belirtilen zafiyetleri bünyesinde barındıran önemli bir tehdit, APT olarak bilinmektedir. Şekilsel olarak ifade edildiğinde bu tehlike daha iyi anlaşılacağı düşünüldüğünden, Şekil 11.1 ile resmedilmiştir. APT'ler ise siber saldırıların en önemlisi ve tehlikeli olanıdır. Bugünün dünyasında gerçek anlamda siber güvenlik ve savunma için bu saldırılar ciddi tehdit oluşturmaktadır. Literatür incelendiğinde "gelişmiş sürekli tehdit" olarak bilinen bu ifadenin, "hedef odaklı saldırı", "ileri düzey sürekli tehdit", "ileri düzey kalıcı tehdit", "ileri düzey saldırı" veya "ileri düzey tehdit" olarakta kullanıldığı, bilindiği veya farklı isimler altında tanımlandığı görülmüştür [3,4]. Kısaca tanımlamak gerekirse bu saldırılar; ileri düzey, özel, kapsamlı ve pek çok yenilikleri, yeni yaklaşımları, planları, projeleri, teknik ve teknolojileri, altyapıları, uzun soluklu hedefleri içerisinde barındıran saldırılara verilen genel isimdir. APT'ler;

- İçerisinde pek çok yenilik, geliştirme, teknoloji, işbirliği, takım çalışması ve operasyonel kullanım gibi çok farklı unsurlar yer alsa da belirli bir hedefe yöneliktir.
- Dikkatli ve sistematik bir çalışmanın ürünü olup, kapsamlı bilgi birikimine, deneyime ve uzmanlığı kullanır.
- İleri düzey bakış açıları içeren, geliştirme veya keşfedilme işlemleri zor ve uzun zaman alan çözümler içerir.
- Üst seviyede motivasyon içerirler.
- İyi bir şekilde kaynak sağlanmış, yüksek yeteneğe sahip ve amansız bir saldırgan grubu tarafından gerçekleştirilen saldırılardır.
- Gizli, hedefli, uyarlanabilir ve veri odaklıdır.
- Devlet destekli olabilecek saldırılar olup, belirli bir hedefi veya odağı olan saldırılardır.



Şekil 11.1. İleri Düzey Kalıcı Tehdit Gösterimi

APT'lerin amacı;

- Hedef varlığı başarılı bir şekilde ele geçirmek,
- Erişimi sürekli tutmak,
- Belirlenen hedefe göre verilere ulaşmak,
- Kurum içerisindeki bir evrakın elde edilmesi ve
- Bir sistemin devre dışı bırakılması, yapılan işlemin amacının anlaşılması veya yönlendirilmesi örnek olarak verilebilir.

Bu saldırı tipini doğru anlamak için kullanılan "ileri düzey sürekli tehdit" ifadesindeki her bir terimi iyi anlamak, ne anlama geldiğini

bilmek, içerisini iyi doldurmak ve tehditin boyutunu anlamak için çok önemlidir. Onun için takip eden başlıklarda bu konulara ağırlık verilmiştir.

11.3. Zafiyetlerin / Saldırıların / Açıklıkların Boyutunu Anlama

Şekil 11.2'de saldırıların yıllara göre değişimi ve gelişimi görülmektedir. Ayrıca, konunun daha iyi anlaşılması için zafiyet, saldırı ve açıklık kelimeleri aşağıda kısaca açıklanmıştır.

Zafiyet; bir yazılım, donanım, sistem, süreç, tasarım ve üretim aşamaları, işletim ve bakım adımlarında kaynaklanan algoritmik, mantık, tasarım, bakım veya test aşamalarında yapılan hatalardan, kurulumlardan, güncellemelerden, değişikliklerden veya yanlış kullanımlardan kaynaklanabilecek ve istismara açık olan hususlara verilen isimdir. Zafiyetlerin, donanım, yazılım ve tasarım kaynaklı olabileceği gibi insan kaynaklı olabileceği de her zaman hatırda bulundurulmalıdır.

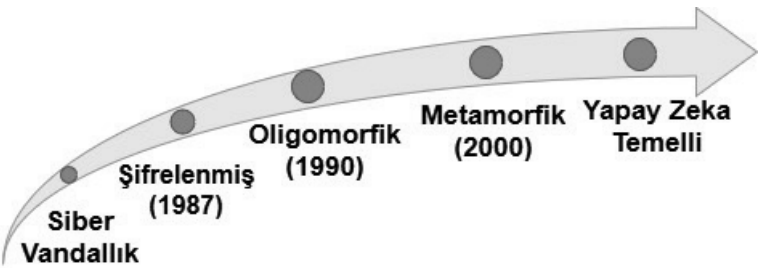
Saldırı; BT sistemlerine veya bu sistemlerdeki hesaplara ve verilere zarar vermek, bu sistemleri durdurmak veya işlemez hale getirmek, sistemlerdeki verileri ele geçirmek, değiştirmek veya yok etmek, sistemleri veya verileri ele geçirip bundan tehdit, şantaj veya sabote ederek menfaat elde etmek amacıyla gerçekleştirilen her türlü girişimdir. Bu saldırılar; solucanlar, trojen, virüs veya zararlı yazılımlar vasıtasıyla yapılabileceği gibi sosyal medya, USB Bellek, e-posta, kullanılan uygulamalar, yüklenen yazılımlar vasıtasıyla olabilmekte ve sistem portları, protokoller, algoritmalar ve yaklaşımlar ile uygulanmayan veya dikkate alınmayan hususları, zafiyetleri veya zayıflıkları kullanılarak yapılabilmektedir.

Açıklık (**Vulnerability**); saldırganların BT sistemlerine erişmek, sızmak, girmek, zarar vermek veya erişim elde etmek için yararlandığı, BT sistemlerinde bulunan zayıflıklar, hatalar veya eksikliklerdir. Açıklıklar, BT sistemlerinin tasarım hatalarından, kullanılan yazılımlarda bulunan eksikliklerden, sistemlerin yanlış yapılandırmasından, farklı sistemlerin entegrasyonundan kaynaklanan problemler veya sistemlerin yanlış veya hatalı yapılandırılmasından kaynaklanabilmektedir.

Bunlara;

- Güncellenmesi yapılmayan bir işletim sistemi, uygulama yazılımı veya koruma yazılımı,
- Kurumun/şirketin kendisinin geliştirdiği veya kullandığı fakat açıklık barındıran bir yazılım,
- Fiziksel güvenliğe önem verilmeyen bir sunucu odası,
- Kurum ağının güvenlik bakış açısıyla tasarlanmaması (kablosuz hizmet veren bir ağa şifresiz erişim),
- BT sistemlerine erişimde kolayca tahmin edilen bir parola kullanma ve
- Kullanılan bilgisayara, akıllı telefonda ekran koruma sistemini aktif hale getirmeme

gibi açıklıklar örnek olarak verilebilir. Son dönemde, kullanıcıların farkındalığının düşük olması sebebiyle saldırganlar tarafından manipüle edilmesi, kandırılması, dolandırılması veya aldatılması kolaylaştığından, kullanıcıların bu zayıflığının kullanılması veya sömürülmesi mümkün olmaktadır. Bundan dolayı ise kullanıcılar sosyal mühendislik saldırılarına maruz kalabilmekte ve bu yaklaşımlar ise kullanılan açıklıklar arasında yer almaktadır. Kısacası kullanıcıların, siber güvenlik ve savunmada en zayıf halka olduğu unutulmamalıdır.



Şekil 11.2. Zararlı yazılımların yıllara göre gelişimi ve değişimi

Siber tehditlerin boyutunu anlatmak için aşağıda bazı önemli görüşler verilmiştir.

- Rusya Devlet Başkanı Sn. Vladimir Putin; internet için "kendi internetimizi geliştirmeliyiz çünkü internetin bir CIA (ABD) projesi" olduğunu belirtmiştir.

- Sn. Binali Yıldırım (T.C. Başbakanı iken); "Siber güvenlik, devletin birinci dereceden ilgilenmesi gereken bir mesele olarak görüyoruz." diye açıklaması bulunmaktadır.
- IBM Yönetim Kurulu Başkanı ve Genel Müdürü. Sn. Ginni Rometty ise "tüm şirketler için en büyük tehdidin siber güvenlik olduğunu" vurgulamıştır.
- Ünlü ve zengin iş adamı Sn. Warren Buffett ise siber güvenliği dünyanın "bir numaralı problemi" olarak görmekte ve siber saldırıların "insanlık için nükleer silahlardan daha tehlikeli" olduğunu belirtmektedir.

Bu tehditlerin boyutunu daha iyi anlatmak için IBM tarafından geliştirilen, DeepLocker isimli yazılımından bahsedelim. Bu yazılım, yapay zekaya sahip "süper zeki kötücül yazılım" olarak tasarlamıştır. Kullanıcıların ses ve yüzlerini gizlice takip ederek en çok konuştukları konuları ve yaptıklarını tespit etmekte ve buna göre dijital reklamlarda oynamalar yapabilmektedir [5]. Google'ın kullanıcıları dinleyerek, akıllı reklam gibi uygulamalarını yöneten Google Asistan uygulamasına benzemektedir. Çalışma prensibi bakımından kötücül bir yazılım gibi çalışan bu ürün, aynı zamanda dikkatsiz kullanıcıların bilgisayarlarındaki açıklıkları tanıyan ve algılayan bir yapıya sahip olup, "püskürt ve af dile (spray and pray)" mekanizması kullanmakta ve hatta pek çok sistemi tespit edilemeden etkileyecek güce sahiptir. Bu kötücül yazılım, kullanıcının bir fotoğrafına ihtiyaç duymakta diğer detayları ise Twitter, Google+ veya LinkedIn gibi sosyal medya ortamlarından almakta ve o kişiyi hedeflemektedir. IBM'deki araştırma ekibi, aygıtların bu yaklaşımdan nasıl etkilendiğini ve DeepLocker'ın etkilerini bir video konferans uygulaması kullanarak göstermişlerdir. Ayrıca araştırma ekibi bu kötü amaçlı yazılımın, anti-casus araçlarının herhangi biri tarafından tespit edilemediğini de göstermiştir. Bu yazılım yapısı incelendiğinde; bu yazılımın 3 katmandan oluştuğu, 1. katmanda hedef sınıf gizlenme, 2. katmanda hedef örnek gizlenme,

3. katmanda ise kötücül yazılım gizlenme gibi amaçları kapsayan yapay zeka temelli çözümleri içerdiği raporlanmıştır.

11.4. İleri Düzey Kalıcı/Sürekli Saldırı Anatomisi

Genel olarak APT saldırılarını incelediğimizde, bu saldırı türünün içerisinde sıfır gün saldırıları bulunan, işletim sistemi ve mimarile-

rinin zafiyetlerini kullanan, sinsice saklanan ve geleneksel metotlar ile bulunamayan, içerisinde casus yazılımlar olabilen, anti-virüs yazılımların tespit etmesinin mümkün olmadığı, ileri düzey teknik ve teknolojileri kapsayan, uzman olmayan kişilerin fark etmesinin mümkün olmadığı, ve son dönemde ise yapay zekâ yaklaşımlarını da içinde barındırdığı bilinmektedir. Bu önemli saldırı türünü anlamak veya iyi anlatmak için açıklamalar aşağıda alt başlıklarda verilmiştir.

11.4.1. Tanımlar ve APT Özellikleri

"İleri düzey" kelimesi, yapılan saldırının gelişmişlik, yüksek bilgi birikimi, yetenek, yenilik ve ileri çalışmaları kapsadığını belirtmektedir. Yani iyi korunan bir ağa bir saldırganın sürekli erişebilecek ve önemli bilgileri ele geçirebilecek özellikte ve yetenekte olduğunu ifade edilmektedir. "**Sürekli/Kalıcı"** kelimesi ise bir tehdidin kalıcı olması, o tehdidin bilgisayar ağına erişimin sürekli olması anlamına gelmektedir. Örneğin, saldırgan bir sisteme erişim sağladığında istediği bilgiye erişene kadar o sistemde kalabilmektedir. "**Saldırı"** kelimesi daha önceki başlıkta detaylı olarak açıklandığı gibi, kişi ve kurumların bilgi varlıklarına izinsiz erişimini ifade etmektedir. Belirlenen hedefe erişmek için yapılan her türlü faaliyeti içermektedir. Saldırganın her zaman kullanılabileceği yeni bir açık, mevcut bir erişim kapısı, kullanılabilecek bir zararlı yazılım, faydalanacağı bir teknolojiyi bulması, bilmesi ve kullanmasıdır [6,7].

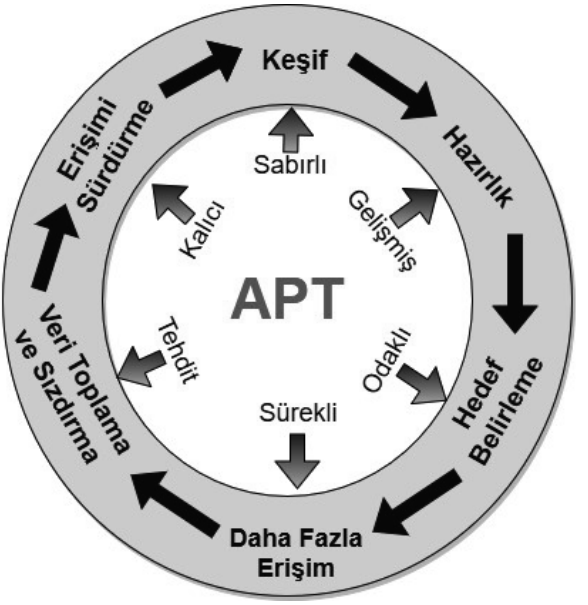
APT'nin genel özelliklerinin bazıları yukarıda verilse de aşağıda daha detaylı olarak verilmiştir. Bunlar;

- Sosyal mühendislik, kötü amaçlı yazılım vb. yöntemlerin kullanımını içerir.
- Saldırı için yeni yöntem veya yaklaşımlara sahiptir.
- Mevcut araç ve gereçlere sahiptir.
- Ekip çalışması yapar.
- Sistemlerin çalışma mekanizmalarını bilir ve açıkları kullanır.
- İleri düzey çalışmalar yapar.
- Gündemi ve açıkları yakinen takip eder.
- Uluslararası bilgi birikimlerinden faydalanır.

- Her türlü saldırı ve saldırgandan faydalanır.
- Derin ve karanlık ağları takip eder.
- Yetenek ve bilgi avcılığı yapar.
- İyi bir laboratuvar ve ya altyapıya sahiptir.
- İleri düzey araştırmacılara sahiptir.
- Fiziksel yaklaşımlar, sosyal yaklaşımlar, tersine sosyal mühendislik gibi yaklaşımları kullanır.
- Sıfır gün saldırıları içerir ve gerektiğinde geliştirir.

11.4.2. APT Genel Yapısı ve Aşamaları

Bir APT'nin genel yapısı Şekil 11.3'de verilmiştir. APT; Keşif, Hazırlık, Hedef Belirleme, Erişim, Veri Toplama ve Sızdırma ile Erişimi Sürdürme adımlarından oluşmaktadır. Bu aşamalar, [8,9] nolu makalelerden derlenerek aşağıda kısaca açıklanmıştır



Şekil 11.3. APT genel işleyişi ([9] nolu kaynaktan esinlenerek geliştirilmiştir.)

- **Keşif** aşamasında; adından da anlaşılacağı gibi, hedefin araştırılması ve keşfi yapılmaktadır ve yapılacak saldırı için hedef veya kurban bilgileri toplanmaktadır. Bu aşamada, çalışma ortamının veya sistemlerinin, konum bilgisi, kullanılan teknolojileri, ileti-

şim kanalları, paydaş bilgileri, ilgi alanları ve adres bilgileri, çalışan bilgileri, zaafiyetler gibi bilgilere ulaşılmaya çalışılmaktadır.

- **Hazırlık** aşamasında, hedefe göre saldırı veya saldırılar planlanır. Senaryolar geliştirilir. Geliştirilen senaryolar test edilir. Sistem açıklarını saptama, kötü amaçlı kod yazımı veya elde edilmesi, uygun donanım ve altyapı seçimi, uygun sosyal mühendislik e-postalarının hazırlanması ve hangi uygun hesaptan gönderileceği, hangi uygun açıklıkların kullanılacağı, saldırı zamanı, diğer saldırı veya açıklıklarla koordinasyon gibi hazırlıkları içerir.
- **Hedef Belirleme** aşamasında, planlanan hususlar gözden geçirilir, yapılan saldırılardan elde edilen bulgular ve izler ele alınır ve hata varsa bunlar düzeltilir veya iyileştirilir. Hedef kapsamında, bir açığı kullanma, bir sunucu bilgisayarı ele geçirme, stratejik bir cihaza USB takma, sosyal mühendislik saldırısı yapma ve amaca ulaşma, bir e-posta gönderme gibi eylemler gerçekleştirilir.
- **Daha Fazla Erişim** aşamasında, sisteme erişim sağladığında saldırganların sistemde kalıcı olması ve daha fazla ağ düğümüne erişimi için yapılması gereken tüm işlemler gerçekleştirilir. Erişilen sistemin veya ağın tanınması, kalıcı olmayı sağlayacak açık kapıların bırakılması, olası durumlarda B ve C planlarının oluşturulması için önceki adımların gerekirse gözden geçirilmesi, aşamalarını kapsar. Ayrıca kötü amaçlı yazılım ve araçların yüklenmesi, sistemlerin detaylı olarak taranması, açıklıkların kayıt altına alınması, sistemlere ve şifrelere erişim gibi işlemler bu aşamada yapılmaktadır.
- **Veri Toplama ve Sızdırma** aşamasında, yukarıda belirtilen hususlar tamamlandığında, saldırı için gerekli olan bilgiler toplanmaya başlanır. Elde edilen bilgiler, bırakılan veya tespit edilen izler, programlar, yöntemler veya araçlar, farklı yöntemler kullanılarak önemli bir yere kayıt edilir veya aktarılır.
- **Erişimi Sürdürme** aşamasında, yapılan saldırı ile hedef sisteme veya yapıya bir kez erişim sağlandığında bu erişimin devam ettirilmesi, bunun sürdürülmesi, gerekli adımların ve yaklaşımların kullanılması gibi adımlar gerçekleştirilir. Ayrıca bu aşama, bırakılan açıklığın veya erişimin tespit edilmesini önlemeye yönelik,

kötü amaçlı yazılımların ve araçların çalışmasını geçici durdurma, minimize etme veya farklı yere yönlendirme, açık bırakılan arka kapıların fark edilmesini engelleme veya açık olanları kullanma, otomatik bilgi toplama ve arama araçları kullanılmışsa bu araçları sistemden gizleme ve hedefe erişmede sürekliliği sağlayacak tedbirleri alma işlemlerini kapsar [8,9].

11.4.3. Siber Saldırılarda APT Rolü

Birçok güvenlik ihlali durumlarında APT anahtar rol oynamaktadır. APT genellikle çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubu olarak ifade edilen rootkitlerin etkin olduğu ve yetkilendirmenin arttırılarak ele geçirilen ağdaki diğer bilgisayarlardaki bilgilerin ele geçirildiği bir yöntemdir. APT saldırılar nadiren pasif olarak fark edilebilmektedir ve bunun için mevcut sistemde aktif ve sürekli devam eden güvenlik ve trafik analizi yapılması gerekmektedir. İnternet ve günümüz şartlarındaki sınırsız ağlardan önce bir saldırgan bir kurumun bilgilerini erişmek istediği zaman bilgilerin saklandığı yere fiziksel erişim yapması gerekiyordu. Fakat günümüzde hassas veriler fiziksel donanıma bağımlı değildirler ve saldırganlar internete bağlı bir cihazla isimsiz olarak uzaktan erişim yapabilmektedirler. Kötücül yazılımlar internet ile birlikte gelişmekte ve saldırganlara için iyi bir saldırı seçeneği olmaktadırlar [10,11,12].

11.4.4. APT Saldırı Kronolojisi

Güvenlik sektör raporları, kamusal duyurular, yapılan yayınlar dikkate alınarak yıllara göre önemli ve kayda değer APT saldırılarının yıllara göre dağılımı Şekil 11.4'de verilmiştir [9,13].

Bu kitabın 10. Bölümünde APT'lerin bazıları kısaca açıklanmış olsa da yıllara göre tespit edilen APT saldırıları bir araya getirilmiş, saldırıların boyutunun ve sayısının giderek arttığını göstermek için Şekil 11.4'de verilmiştir. Şekilde verilen saldırılara birer örnek aşağıda kısaca açıklanmıştır.

MOONLIGHT MAZE - 2000

Moonlight Maze adı verilen siber saldırı, Pentagon, Nasa ve Birleşik Devletler Enerji Bakanlığı, araştırma laboratuvarları ve özel üniver-

sitelere ait bilgisayarları hedef almıştır. Güvenlik uzmanlarının bu saldırı ile ilgili tespiti Mart 1998'de olmuştur. Ulusal Altyapı Koruma Merkezinden sorumlu bir yetkili, saldırının Rusya merkezli olduğunu ifade etmiştir. Saldırı sonrasında Pentagon şifreleme ve saldırı tespit sistemlerini güncellemek için 200 milyon dolar bütçe ayırmıştır [14].

Şekil 11.4. APT Saldırılar ve Tespit Yılları

US CONGRESSMAN - 2006

İki kongre üyesine ait bilgisayar ele geçirilmiş olarak raporlanmıştır. Çalınan bilgilerin kritik bilgiler olup Çin-Pekin rejimine karşı muhaliflerle ilgili olduğu bildirilmiştir [9].

OAK RIDGE - LOS ALAMOS NATIONAL LABORATORY - 2007

Oak Ridge National Laboratory yapılan saldırılar başarılı bir şekilde sosyal mühendislik epostaları ile gerçekleştirilmiş ve eposta yoluyla yapılan yazışmalar yasal bir şekilde yürütülmüştür. Tesisi ziyaret eden ziyaretçilere ait bilgilerin bulunduğu bilgisayarlar ele geçirilmiştir. Saldırganların veri tabanındaki tüm bilgileri çaldıkları tahmin edilmektedir Los Alamos National Laboratory bütün müşterilerine tanımlanamayan "Sarı" ağda etkilenmiş küçük sayıdaki bilgisayarlara gönderilen kötü amaçlı bir eposta için uyarması ile ortaya çıkmıştır. Önemli miktarda sınıflandırılmamış veri çalınmıştır. Saldırının geniş çapta ve koordineli olarak Birleşik Devletler enstitü ve laboratuvarlarını hedef aldığı düşünülmektedir [9].

STUXNET - 2010

Literatüre hedefli ilk saldırı olarak geçen Stuxnet solucanı, İran'ın Natanz kentinde bulunan nükleer santralin uranyum zenginleştirme tesisini hedef almış, 2010'da tespit edilen bir saldırıdır. Stuxnet solucanı bir USB bellek ile Natanz tesislerindeki bilgisayarlara bulaştırılmış ve bu solucan kendini kopyalayarak çoğalmıştır. PLC kullanan ve gerçek zamanlı veri toplama, kontrol ve izleme yapan SCADA sistemleri etkileyerek zenginleştirmede kullanılan santrifüjlerin devre dışı kalmasına ve hatalı çalışmalarına yol açmıştır. İçerisinde sıfır gün saldırılarını da barındıran bu saldırı, dünya literatüründe kapsamlı olarak araştırılmış ve bundan çok iyi dersler çıkartılmış bir saldırı olarak tarihe geçmiştir [15].

DUQU- 2011

2011 yılında keşfedilmiştir. Şubat 2010'dan beri aktif olduğu tahmin edilmekte ve yeni versiyonları bulunmaktadır. Stuxnet ile oldukça benzerlik gösteren Duqu için, aynı saldırganlar tarafından geliştirildiği fakat farklı hedefler için kullanıldığı belirtilmektedir. Duqu saldırısında temel hedefin casusluk olduğu, Microsoft Word dosyasında bulunan True Type font açığından yararlanarak sıfır gün saldırısı yapıldığı, hedef aldığı bilgisayarı bir sonraki hedef için kul-

landığı, klavye kaydedici (keylogger) ile elde edilen verileri XOR yöntemiyle de şifrelediği gibi hususlar literatürde mevcuttur. Bu saldırı türünün üç farklı sıfır gün açığından faydalanan Duqu 2.0 versiyonu da gelişmiş kötücül yazılımlar kullanmıştır. Rusya, ABD, Çin, Fransa, İngiltere ve Almanya gibi ülkelerin birlikte yaptığı faaliyetleri takip etmeyi amaçlamıştır. [16].

FLAME - 2012

İlk olarak Mayıs 2012'de keşfedilen Flame saldırısının 5-8 yıldan beri aktif olduğu tahmin edilmektedir. Başka tür saldırılar araştırılırken tesadüfen keşfedilmiştir. Bu saldırıda kullanılan kötücül yazılıma ait en ilginç özellik, tüm modülleri ile birlikte yaklaşık 20 Megabayt civarında bir büyüklüğü olmasıdır. Flame ile Stuxnet ve Duqu arasında çok güçlü bir bağ kurulamasa da genel kod yapısı ve fonksiyonları benzerlik göstermektedir. Bu yüzden Stuxnet ve Duqu saldırılarını gerçekleştiren aynı saldırganların değil fakat işbirliğinde olan saldırganların yaptığı tahmin edilmektedir. Flame, Duqu'ya benzer olarak bilgi sızdırmayı hedeflemiş ve bunu Ortadoğu'daki ülkeler başta olmak üzere binlerce Windows tabanlı sisteme yayarak çok geniş alanda yapmıştır. Büyük ve karmaşık bir yapıya sahip olan Flame kötücül yazılımı USB belleklerle yerel ağlarda yayılması için tasarlanmıştır. Kendini çoğaltma yeteneği olmayan kötücül yazılımlar için saldırgan iki farklı sıfır gün (Yazıcı Kuyruğu ve Windows Shell) açığını kullanarak başka bilgisayarları etkilemesini sağlayabilmektedir. Flame saldırısında C&C sunucu için 80'den fazla domain kullanılmış olup şifreleme tekniği olarak XOR şifreleme ve RC4 algoritmaları kullanılmıştır [16].

TEAMSPY - 2013

Siber tarama faaliyetlerini kapsayan TeamSpy saldırısı Bağımsız Devletler Topluluğu ve doğu Avrupa ülkelerindeki yüksek seviyedeki politikacıları ve insan hakları örgütlerini hedef almıştır. Saldırgan kurban bilgisayarları yasal dijital sertifikası olan ve yüz milyondan fazla kullanıcısı bulunan TeamViewer uzaktan erişim programı ile kontrol etmiştir. Bir tarama ve veri sızdırma operasyonu olan TeamSpy kurbanlarından klavye hareketleri ve ekran bilgilerini, gizli şifre ve içerikleri, ITunes programı ile Apple cihazların geçmişi gibi bilgileri sızdırmıştır. Saldırının belirtilen ülkelerde hala aktif olduğu düşünülmektedir [17].

EQUATION - 2014

Equation grubu çok yönlü, tam donanımlı ve şimdiye kadar görülen en tehlikeli saldırgan grup olarak tanımlanmaktadır. Bu saldırgan grup, kullandıkları şifreleme algoritmaları, gizlenme stratejileri ve saldırı esnasında kullandıkları gelişmiş teknikler ile dikkat çekmektedir. Kullandıkları kötü amaçlı yazılımlar için çeşitli isimlendirmeler yapılmış olup GrayFish, Fanny ve EquationDrug öne çıkan yazılımlardır. Equation grubu saldırıları gerçekleştirirken kendini çoğaltabilen solucandan (Fanny), CD-ROM gibi fiziksel medya aygıtlarından veya web tabanlı açıklardan yararlanmaktadırlar. Kullandıkları şifreleme algoritmaları RC5,RC6 ve XOR şifreleme teknikleridir. İran, Rusya, Pakistan başta olmak üzere 30'un üzerinde ülkede faaliyet göstermektedirler. Hedeflerinde hükümet ve diplomatik kurumlar, telekomünikasyon sistemleri, nükleer enerji, doğalgaz üretim ve askeri tesisler vardır [18].

DUQU 2.0 - 2015

2011 yılında ortaya çıkan ve 2012 yılında durağan hale geçen Duqu saldırısının gelişmiş bir versiyonu olarak tanımlanmaktadır. Üç adet sıfır gün açığından faydalanan Duqu 2.0 saldırısında gelişmiş kötücül yazılımlar kullanılmıştır. Şimdiye kadar olan tüm saldırılardan farklı bir süreklilik mekanizması olan bu saldırının sadece bilgisayar hafızasında kod gizleme özelliği tespit edilebilmiştir. BM daimi üyesi beş ülke olan Rusya, ABD, Çin, Fransa ve İngiltere'nin yanı sıra Almanya'yı kapsayan P5+1 olarak adlandırılan ülkelerin birlikte yaptığı faaliyetleri hedef almıştır. Duqu 2.0 saldırısının gelecekteki tüm APT saldırılar için örnek teşkil edeceği düşünülmektedir [19].

LAZARUS - 2016

Adını Sony Pictures ve bir grup finans kurumuna saldırması ile duyuran Kuzey Koreli hacker grubu Lazarus, Kaspersky firması tarafından tespit edilmiştir. Bu grup ilk büyük saldırısını Bangladeş Halk Cumhuriyeti Merkez Bankasına yapmış ve bankaya 81 milyon dolar zarar vermiştir. Bununla da yetinmeyen saldırganlar, sonrasında kripto para sahiplerini hedef almışlardır. Kurbanlarının hesap cüzdanlarını elde etmek için kripto para değişimi yapan şirketlerin ağına kötücül yazılım yerleştirmişlerdir. Bilgisayar ağına sızma bir e-posta ile başlamakta ve bir kripto para uzmanı çalışa-

na "Celas Trade" adında ticari bir uygulamayı indirmesi için link göndermektedir. Bu link ile programı yükleyen çalışan arka kapı saldırısına maruz kalmış olup şirketin ne kadar zararda olduğu tam olarak bilinmemektedir [20].

WANNACRY - 2017

İspanya'nın Bilgisayar Acil Müdahale Ekibi CCN-CERT, birkaç İspanyol kuruluşunu etkileyen büyük bir fidye yazılımı saldırısı hakkında sitelerinde bir uyarı yayınlaması ile ortaya çıkan WannaCry saldırısı, kötücül bir yazılım ile hedef bilgisayardaki dosyaları şifrelemektedir. Şifrelemenin kaldırılmasını için saldırganlar, bilgisayar başına 600 dolar para talep etmiştirler. Saldırıda ayrıca İngiltere'deki Ulusal Sağlık Servisi (NHS)'ne bağlı 16 sağlık kurumu etkilenmiş, Rusya, Ukrayna ve Hindistan da dâhil olmak üzere 74 ülkede 45.000 in üzerinde saldırı meydana gelmiştir [21].

OCTOPUS - 2018

DustSquad saldırı grubu tarafından yapılan ve adına Octopus denilen siber casusluk saldırısı Orta Asya kullanıcılarını ve diplomatik varlıkları hedef almıştır. İlk olarak ESET firmasının kullandığı Octopus ismi saldırganların 0ct0pus3.php betik dosyasını kullanmasından ileri gelmektedir. Saldırı için Delphi programını kullanan DustSquad grubunun 2014 yılından bu yana Rus dilini konuşan eski Sovyetler Birliği ülkeleri ile Afganistanı hedef aldığı tahmin edilmektedir [22].

11.5. APT'lere Karşı Savunma Yaklaşımları

APT saldırılardan korunmak için birçok kurum ve kuruluş yüksek seviyede savunma stratejisi uygulamaktadır. Her zaman dikkat edilmesi gereken nokta, korunmanın ideal olduğu fakat tespit sisteminin mutlaka gerektiğidir. Kurumların çoğu sadece önleyici tedbirler üzerinde durmaktadır fakat APT saldırılarının esas problemi kötü niyetli kişinin sisteme dâhil olması ve trafik akışını hissettirmeden izlemesidir. APT saldırılara karşı alınabilecek tedbirler şu şekilde sıralanabilir [23].

11.5.1. Kullanıcıları Kontrol Etmek Ve Farkındalığı Arttırmak

Genel kural şudur; bilinçsiz kullanımı engelleyemezsiniz fakat bilinçsiz kullanıcıyı kontrol altına alabilirsiniz. Birçok saldırgan kulla-

nıcıların bir eposta eklentisini açması ile ya da tıklamaması gereken bir bağlantıyı tıklaması ile ağa sızmaktadır. Tam bir farkındalık yaratmak ve kullanıcının hareketleri kısıtlama ile tehlikeler azalacaktır. Saldırganın keşif tarama süreci içerisinde yer alan kullanıcı avlama teknikleri, ağı kullanan kişi veya çalışanların bilinçlendirmesi ile önlenebilmektedir [23,24].

11.5.2. İsim Oylama Yöntemini Ağ Davranışlarında Yürütmek

Geleneksel güvenlik çözümleri ağ içerisindeki davranışları iyi-kötü olarak sınıflandırmakta ve sonrasında erişime izin vermekte veya engellemektedir. Fakat gelişmiş ataklarda sınıflandırma yöntemi işe yaramamaktadır. Birçok saldırgan ağ içerisinde meşru davranarak ağ içerisinde şüphe çekmezler. Bu yüzden saldırganın ağa karışma hedefinden dolayı ağ içerisindeki hareketler için bir güven seviyesi belirlenerek kullanıcılara oy verme yöntemi uygulanabilir ve oylama mekanizmasının üreteceği güven değeri ile bir IP adresinin kötü amaçlı DNS ve trafik vektörlerinden etkilenip etkilenmediği belirlenebilir [23,25].

11.5.3. Değişen Saldırıları Anlamak

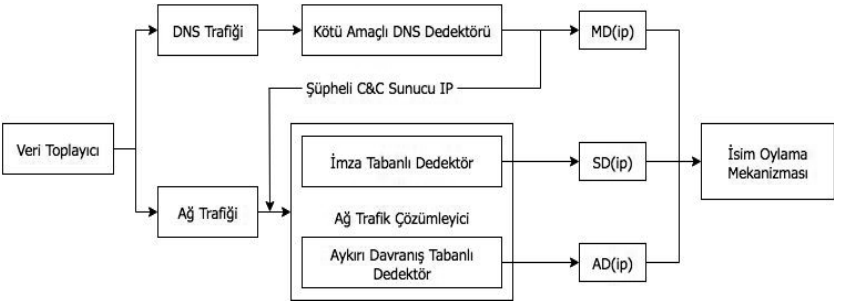
Bilinmeyen bir tehdide karşı savunmak yapmak oldukça zordur. Bu nedenle iyi bir savunma yapabilmek için saldırıyı iyice anlamak ve nasıl yürütüldüğünü bilmek gerekir. Eğer kurumlar yeni teknikleri ve saldırganların geliştirdikleri metotlarını anlamaya çalışmazlarsa savunma mekanizmalarını doğru ve etkin bir şekilde ayarlamazlar [23]. Dolayısıyla siber güvenlik uzmanları, geçmiş yıllarda meydana gelen ve tespit edilen APT saldırıların analiz edildiği ve raporlandığı kaynaklardan faydalanmalıdırlar. Bu noktada, Ulusal Güvenlik Arşivi isimli web sitesi bu kaynaklara iyi bir örnektir. Bu sitede APT saldırıları, etkilenen ülkeler, hedefler, saldırı türleri derlenmekte ve Siber Savaş Haritası (CyberWar Map) olarak görselleştirilmektedir [26]. CyberWar Haritası, Ulusal Güvenlik Arşivinin Cyber Vault Projesinin bir parçası olarak devlet-devlet siber çatışmalarında öne çıkan oyuncuların ve olayların bazıları için görsel bir rehberdir. Bu kaynak devlet destekli siber saldırılara odaklanmaktadır. Haritanın güncel versiyonlarına, Siber Vault Projesi ana sayfasından erişilebilir [27].

11.5.4. Son Noktayı Yönetmek

Saldırganların ağa bir başlangıç noktasından girmesiyle istediği bilgiye son noktada erişmektedir. Eğer zarar azaltılmak isteniyorsa hedeflenen son noktayı kontrol altına almak veya geçici olarak kilitlemek uzun süreli bir koruma sağlayacaktır [16,23].

11.5.5. Ağın Tüm Trafiğine Odaklanmak

Mevcut ağ sistemin tüm trafiğinin izlenmesi APT saldırıları tespit etmek için etkin bir yöntemdir. Bunun için birçok makine öğrenme algoritması ve birçok modelleme belirli ağ özelliklerini ayırt etmek için kullanılmaktadır. Bilinen ataklar için imzaya dayalı tespit sistemi, ağda normal davranışlar dışında dağılım gösteren hareketleri tespit etmek için kullanılan olağan dışı durum tespit sistemi ve bu iki sistemin birleştirilerek kullanıldığı hibrit sistemler APT tespiti için uygulanabilmektedir. Ayrıca geliştirilen ihlal tespit sistemleri ile mevcut ağ DNS ve Ağ trafiği olarak ikiye ayrılmaktadır ve ağ trafiğinin uç yapılarında çalışarak bilinmeyen saldırıları da belirli özniteliklere dayanarak yakalayabilmektedir [24,25]. Örnek bir tespit sistemi Şekil 11.5'de verilmiştir.



Şekil 11.5. APT Tespit Sistemine bir örnek [25]

Literatürde mevcut saldırılara bakıldığında, önemli ve kayda değer pek çok APT saldırıları mevcuttur. Bunların sayıları ve gelişimine bakıldığında son dönemde bu saldırıların ciddiyeti ve verebileceği zararlar pek çok ulusu etkileyebilecek düzeydedir ve ciddi önlemler alınmalıdır. Yeni nesil saldırıları anlama ve bunlardan korunmak için mutlaka kapsamlı bilgiye sahip olunması, deneyimli ve yetenekli ekiplere ihtiyaç olduğu, altyapı ve araçlara sahip olunması gerektiği, yeni nesil teknik, teknoloji ve yöntemlerin bilinmesi ve uygulanması ve üzerinde sürekli çalışılması gereklidir.

11.6. Değerlendirmeler

Bu bölümde kısaca açıklanan detaylardan, verilen bilgilerden ve yapılan açıklamalardan açıkça görülebileceği gibi APT saldırılar, günümüzde faaliyetlerini elektronik ortamda sürdüren kurum ve kuruluşlar ve en önemlisi ise ülkeler için büyük tehlike arz etmektedir. Bu tür saldırıların gelecek yıllarda daha da artacağı, yeni ve farklı şekilde karşımıza çıkacağı kesindir. Bu saldırılara genel olarak bakıldığında bu tür saldırıların;

- Hedefli ve odaklı olduğu,
- Önemli ve stratejik hedeflere yapıldığı,
- Son derece organize olduğu,
- Arkasında doğrudan olmasa da dolaylı olarak büyük devletlerin olabileceği,
- Saldırı motivasyonun yüksek olduğu,
- Hedefe başarı ile ulaşılması için yeterli kaynağa sahip olunduğu,
- Üst düzey eğitimli ve yetenekli uzmanların bu saldırıları planladığı ve uyguladığı
- Sabırlı ve uzun soluklu saldırıları içerdiği

bilindiğinden, bu ve buna benzer saldırılardan korunmak çok farklı bilgi birikimine, deneyime, uzmana, gelişmiş araçlara, iyi bir koordinasyona ve en önemlisi ise maddi desteğe ve aşağıda verilen maddelerde kısaca özetlenen hususların dikkate alınması gerekmektedir. Bunlar:

- Öncelikle Bölüm 11.5'de açıklanan APT'lere karşı savunma tedbirleri dikkate alınmalı ve uygulanmalıdır.
- Kurumsal ve kritik altyapılara sahip yapılar için bu saldırılar önemsenmeli, saldırıların geleneksel saldırılardan farklı olduğu bilinciyle hazırlıklar yapılmalı, sistemler araştırılmalı, önlemler alınmalı, konuya kaynak ayrılmalı, ön hazırlıklar ve çalışmalar yapılmalıdır.
- Saldırıları önlemede kullanıcıları/çalışanları bilinçlendirmek ve farkındalık oluşturma önemlidir. Mesela, bilinmeyen e-postaları açmama, linklere tıklamama, yazılım güncellemelerini zamanın-

da yapma alınabilecek en basit önlemlerdir. Bu ve buna benzer çözümler geliştirilmeli ve uygulanmalıdır.

- Bu saldırılar, içerisinde pek çok saldırı türünü içerse de en önemlisi sıfır gün saldırılarıdır. Çoğu zaman fark edilemez durumda olan bu tehditlerden korunmak ancak ve ancak yüksek bilgi birikimine sahip, yetenekli ve bu hususlarda çalışan uzmanlar, uluslararası tehdit listelerini takip, özellikle bu saldırıları tespit eden firma uyarılarını yakından izleme, USOM'dan destek alma, ilgili kurumlarla işbirliği ile aşılabilecek konulardır.
- Kurum ve kuruluşların kendi ağ ve bilgi sistemlerini iyi bir şekilde tanımaları ve yönetmeleri, kurum ağ trafiğini ve hizmetlerini sıkı bir şekilde takip etmeleri gerekmektedir.
- Şüpheli durumlar Ulusal Siber Olaylara Müdahale Merkezine (USOM) anında bildirilmeli ve destek istenilmeli, alınacak önlemler ve tespit edilen zafiyetlerin ivedilikle giderilmesine yönelik aksiyon planları hazırlanmalı ve hayata geçirilmelidir.
- Üniversitelerde APT'leri anlama, tespit etme ve karşı koyma yeteneklerini geliştirici araştırmalar ve tezler yaptırılmalı, kişisel, kurumsal ve ulusal birikimler arttırılmalıdır.
- Konu ile ilgili yetenek geliştirici seminerler, konferanslar, etkinlikler veya çalışmalar yapılmalıdır.
- Sunulan bilgilerden de görülebileceği gibi bazı ülkelerin APT geliştiren takımlarının bulunduğu, geliştirilen APT'leri sayılarla ifade ettikleri, bazı saldırıların ise düşman sistemlerini ele geçirmeye yönelik çalışmaları içerdiği bunu doğrudan ifşa etmedikleri de ayrıca bilinmektedir. Sonuç olarak, konunun ciddiyetinin farkında olunarak çalışmalar yürütülmelidir.
- Hedef olacak veya olabilecek sistemler, bu bakış açısıyla kurulmalı, izlenmeli, denetlenmeli ve gözden geçirilmeli, anormal durumların üzerinde titizlikle durulmalı, şüpheli durumlar iyice araştırmalı ve sonuçlandırmalıdır.
- Ülkemizde APT konusunda yapılan akademik ve sektörel çalışmaların çok az olduğu, ülkemizde tespit edilen ve kamuoyu ile paylaşılan bir APT bulunmadığı/bulunamadığı, yapılan çalışmaların ise gerçek bir APT olduğunu gösterir net bulguları içerme-

diği belirlenmiştir. Bu hususlara daha çok önem verilmeli, bu konuda yetenek geliştirmenin yanında milli ürünlerin geliştirilmesi de özendirilmelidir.

- Cumhurbaşkanımızın TÜBİTAK ve TÜBA Ödülleri Töreni'nde yaptığı konuşmada bahsettiği Ahtapot yazılımının siber güvenlikte üstlendiği role işaret ederek "Bugün siber saldırılar ve açıklar, devletin güvenliği ile kişi mahremiyetini ihlal eden en büyük tehditlerdendir. Geliştirdiğimiz 'Ahtapot' yazılımı, bir kuvvet komutanlığımızın karargahına yapılan siber saldırıyı başarıyla engelledi ve gerçekleşecek bir NATO tatbikatına dahil edildi" ifadesi önemli ve sevindirici bir açıklamadır. Ülkemizde APT'lere karşı yapılacak mücadele için en iyi örnektir. Bu gibi başarı hikâyelerinin sayısının artırılması gereklidir.
- APT saldırılarının amacı, kapsamı, boyutu ve hedefi değerlendirildiğinde, bu saldırılara karşı koyabilmek için ulusal APT araştırma merkezi kurulmalı, bu merkezde değerlendirme bölümünün başında belirtilen hususları önlemek için çalışmalar yürütülmektedir.
- Yapılan güncel araştırmalar bizlere, APT saldırılarının bilindiğinden ve Şekil 11.4'de sunulan saldırılardan sayısının daha fazla olduğu bir kez daha göstermiştir. Günümüzde yapılan ve gelecekte daha da şiddetlenecek olan saldırılara karşı ülkelerin tabii ki başta ülkemizin ulusal ve uluslararası ortak çözümler üretmesi gerekmektedir.
- APT saldırıların özellikle odaklı ve hedefli olduğu bilinse de bu tür saldırıların bazı sistemlere, kurumlara veya uluslara yapıldığı bilinciyle hareket edilmeli, her ülkenin bu tehditlere her zaman maruz kalabileceği unutulmadan hazırlık yapılmalı ve önlemler alınmalıdır.
- AB ülkeleri arasında konuyla ilgili olarak işbirliği yapılmasının zor olduğu veya bunun gerçekleştirilmesinin şu an için imkansız olduğu düşünülse de gelecekte buna çok ihtiyaç duyulacağı değerlendirildiğinden bugünden bilgi paylaşımı ve işbirliği yapılabilecek ortamlar için girişimlerde bulunulmalıdır.

Kaynaklar

[1] Akın, M., Sağıroğlu, Ş., "Gelişmiş Sürekli Tehditler", *in 9th International Conference On Information Security and Cryptology (ISC TURKEY 2016)*, Ankara, Türkiye, 2016, pp.79-87.

[2] Akın M., Sağıroğlu Ş., "Gelişmiş Sürekli Tehditler", Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, vol. 10(1), pp.1-10, 2017.

[3] J. Chen, C. Su, K. Yeh and M. Yung, "Special Issue on Advanced Persistent Threat", *Future Generation Computer Systems*, vol. 79, pp. 243-246, 2018. Available: 10.1016/j.future.2017.11.005 [Erişim: 08 Mart 2019].

[4] A. Lemay, J. Calvet, F. Menet and J. Fernandez, "Survey of publicly available reports on advanced persistent threat actors", *Computers & Security*, vol. 72, pp. 26-59, 2018. Available: 10.1016/j.cose.2017.08.005.

[5] İnternet: "DeepLocker Concealing Targeted Attacks with AI Locksmithing", URL: https://web.archive.org/web/20190321112747/https://i.blackhat.com/us-18/Thu-August-9/us-18-Kirat-DeepLocker-Concealing-Targeted-Attacks-with-AI-Locksmithing.pdf [Erişim: 21 Mart 2019].

[6] M. Auty, "Anatomy of an advanced persistent threat", *Network Security*, vol. 2015, no. 4, pp. 13-16, 2015. Available: 10.1016/s1353-4858(15)30028-3 [Erişim: 8 Mart 2019].

[7] Bayrak M.E., "Gelişmiş Kalıcı Tehdit Saldırılarının Ağ Akış Analiziyle Tespit Edilmesi", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2015.

[8] R. Brewer, "Advanced persistent threats: minimising the damage", *Network Security*, vol. 2014, no. 4, pp. 5-9, 2014. Available: 10.1016/s1353-4858(14)70040-6.

[9] İnternet: "Advanced Persistent Threats: A Decade in Review", URL: https://web.archive.org/web/20190321114535/https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2011/C5_APT_ADecadeInReview.pdf [Erişim: 21 Mart 2019].

[10] D. Denning, "Framework and principles for active cyber defense", *Computers & Security*, vol. 40, pp. 108-113, 2014. Available: 10.1016/j.cose. 2013.11.004.

[11] A. Sood and R. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats", *Security & Privacy*, IEEE, vol.11, pp. 54-61, 2013.

[12] G. Thomson, "APTs: a poorly understood challenge", *Network Security*, vol. 2011, no. 11, pp. 9-11, 2011. Available: 10.1016/s1353-4858(11)70118-0.

[13] C. Raiu, "Cyber-threat evolution: the past year", *Computer Fraud & Security*, vol. 2012, no. 3, pp. 5-8, 2012. Available: 10.1016/s1361-3723(12)70051-9.

[14] İnternet: Llongueras A., "Moonlight Maze The beginning of a new era", URL: https://web.archive.org/web/20190321114710/https://www.academia.edu/6182336/MOONLIGHT_MAZE._The_beginning_of_a_new_era [Erişim: 21 Mart 2019].

[15] Shakarian P., Shakarian J. and Ruef A., "Attacking Iranian Nuclear Facilities: Stuxnet" in *Introduction to cyber-warfare*, Waltham, MA: Syngress-Elsevier, 2013, pp.224-235.

[16] Virvilis N., Gritzalis D., Apostolopoulos T., "Trusted Computing vs. Advanced Persistent Threats : Can a Defender win this game", in *2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE 10th International Conference on Autonomic & Trusted Computing*, Vietri sul Mare, Italy, 2013, 396-403.

[17] İnternet: "The TeamSpy Crew Attacks - Abusing TeamViewer for Cyberespionage", URL: https://web.archive.org/web/20190321115242/https://securelist.com/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/35520/ , [Erişim: 21 Mart 2019].

[18] İnternet: "Equation Group: Questions and Answers", URL: https://web.archive.org/web/20190321120322/https://www.a51.nl/sites/default/files/pdf/Equation_group_questions_and_answers.pdf, [Erişim: 21 Mart 2019].

[19] İnternet: "The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns", URL: https://web.archive.org/web/20190321120516/https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/ [Erişim: 21 Mart 2019].

[20] İnternet: "A cryptocurrency exchange hack with a North Korean accent", URL: https://web.archive.org/web/20190321120839/https://www.kaspersky.com/blog/lazarus-crypto-exchange-attack/23610/ [Erişim: 21 Mart 2019].

[21] İnternet: "WannaCry ransomware used in widespread attacks all over the world", URL: https://web.archive.org/web/20190321121051/https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/ [Erişim: 21 Mart 2019].

[22] İnternet: "Octopus-infested seas of Central Asia", URL: https://web.archive.org/web/20190321121253/https://securelist.com/octopus-infested-seas-of-central-asia/88200/ [Erişim: 21 Mart 2019].

[23] Cole E., "The Changing Threat" in *Advanced Persistent Threats Understanding the Danger How to Protect Your Organization*, Waltham, MA:Syngress-Elsevier, 2013, pp.20-26.

[24] De Vries J.A., "Towards a roadmap for development of intelligent data analysis based cyber attack detection systems", MSc Thesis, Delft University of Technology, Technology Policy & Management, Delft, Hollanda, 2012.

[25] G. Zhao, K. Xu, L. Xu and B. Wu, "Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis", *IEEE* Access, vol. 3, pp. 1132-1142, 2015. Available: 10.1109/access.2015.2458581 [Erişim: 08 Mart 2019].

[26] İnternet: "APT Index / Default View Kumu", URL: https://web.archive.org/web/20190321122258/https://embed.kumu.io/0b023bf1a971ba32510e86e8f1a38c38 [Erişim: 21 Mart 2019].

[27] İnternet: "The Cyber Vault Project / National Security Archive", URL: https://web.archive.org/web/20190321123126/https://nsarchive.gwu.edu/project/cyber-vault-project [Erişim: 21 Mart 2019].

Sızma Testleri

BÖLÜM 12

Dr. Adem TEKEREK - Dr. Yılmaz VURAL

SIZMA TESTLERİ

Bu bölümde; sızma testleri, türleri, sızma testine karşı zafiyet değerlendirmesi, güvenlik testi metodojileri, test aşamaları, ile güvenlik testi etiği gibi konular kapsamlı olarak açıklanmış ve konu sonuçta siber güvenlik açısından değerlendirilmiştir.

12.1. Giriş

Bilgi sistemlerindeki zayıflıkları ve eksiklikleri tanımlamanın en etkili yöntemlerinden olan sızma testleri potansiyel güvenlik ihlalleriyle ilişkili risklerin değerlendirilmesi amacıyla erişim, yetkilendirme ve işlevsellik amaçlı sistemlere zarar verilmeden yapılan gerçek saldırıların simüle edilmesini sağlar. Sızma testleriyle güvenlik amaçlı alınan önlemlerin yeterli olup olmadığı ve zafiyet ve zayıflıkların saldırıya açık olup olmadığı ortaya konularak keşfedilen güvenlik açıklarının raporlanması ve giderilmesi amacıyla çalışmalar yapılır. Siber saldırılar incelendiğinde saldırganların genellikle var olan güvenlik açıklıklarını kullanarak saldırılarını gerçekleştirmesi sızma testlerinin önemini ortaya koyar. Sızma testleriyle güvenlik sorunlarının saldırganlardan önce bulunarak nasıl düzeltileceği ve muhtemel güvenlik açıklarına karşı nasıl önlem alınacağı konusunda önlemler alınması sağlanır [1].

Sızma testleri, nitelikli güvenlik uzmanları tarafından, hedeflenen bilgisayar ağı veya uygulama hakkında bilgi sahibi olmadan ve kısmi olarak bilgi sahibi olarak, iç ağdan veya dış ağdan gerçekleştirilir. Testler uygulamalar, bilgisayar ağ cihazları, işletim sistemleri, iletişim araçları, fiziksel güvenlik ve insan faktörü olmak üzere bütün bilişim altyapısını kapsayacak şekilde planlanır. Sızma testinin sonunda, testi yapılan hedef ortamın ve ortamda bulunan zafiyetlerin ve çözüm önerilerinin bulunduğu sızma testi raporu oluştu-

rulur. Sızma testleri sırasında, metodolojik bir süreç kullanılır ve test sürecinin her aşamasında tespit edilen zafiyetlere göre, çözüm üretilmesi gereklidir. Tespit edilen her bir zafiyet için oluşturulan çözüm önerisi de raporlanarak, testi yaptıran kuruma teslim edilmelidir [2].

Yüksek seviyede bilgi güvenliğinin sağlanmasında önemli bir rol oynayan sızma testleri kişisel verilerin korunması ile ilgili yasal düzenlemeler kapsamında önemli bir konu haline gelmiştir. Gerek ülkemizde yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) gerekse Avrupa'da yürürlükte olan Genel Veri Koruma Tüzüğü (GDPR) kapsamında veri sorumluları veri güvenliğinin sağlanması ile ilgili idari ve teknik tedbirleri almakla yükümlüdür. Bu düzenlemelerin en önemli yönlerinden birisi, veri güvenliğinin sağlanamaması sonucunda meydana gelecek muhtemel bir ihlalin saldırıya uğrayan ve kişisel verilerin güvenliğini sağlayamayan işletmelerin büyük cezalarla karşı karşıya kalmasıdır. Bu kapsamda sızma testleri, kişisel verilerin işlendiği bilişim sistemlerinin güvenliğinin sağlanmasına ilişkin risklerin yönetilebilmesi amacıyla bilişim sistemlerinin değerlendirilmesi ve güvenlik kontrollerinin etkinliğinin düzenli olarak test edilmesi açısından önemli bir rol oynar.

2018 yılı içerisinde yaşanan yüksek düzeyli saldırılar incelendiğinde (Equifax, WannaCry, vb.) bu saldırıların şirketlere çok yüksek maliyetleri olmuştur. Siber saldırıların her geçen gün çeşitlenerek devam ettiği günümüzde sızma testlerinin istenen sonuçları verebilmesi amacıyla yeni tehdit ve zafiyetlerin de dikkate alınması gerekmektedir. Saldırganların yeteneklerini her geçen gün geliştirmesi siber güvenlik sistemlerinin tehditlere karşı korunmalarını zorlaştırmakta ve hangi güvenlik alanlarına yatırım yapılması önemli hale gelmektedir. Sızma testleri ile güvenliğin sağlanmasındaki en zayıf olan noktalar açığa çıkarıldıktan sonra, doğru alanlara yatırım yapılması ihlallerin yaşanmasını önler veya etkilerini en az seviyeye indirir. Sızma testlerinin bir diğer önemli faydası ise bilgi güvenliğinin dışarıdan farklı bir bakış açısı ile sınanmasıyla mevcut uzmanların geliştirmesi gereken yönlerini de ortaya çıkararak alınması gereken eğitimlerin doğru seçilmesinde etkin rol oynar [3].

Sızma testlerinin kapsamı teknolojilere ve uygulamalara göre farklılık gösterebilir. Tüm bilişim sistemlerinin sınanmasına ek olarak işletmeye özgü kritik alanlara (Ağ testi, Mobil Uygulama Testi, Web Uygulama Testi, Bulut Testi, Sosyal Mühendislik Testi, vb.) ayrıca odaklanılabilir. Sızma testleri farklı kapsam veya araç setlerine sahip olarak yapılsa da ortak bir metodolojiyi paylaşırlar. Sızma testleri kara kutu, beyaz kutu ve bu iki yöntemin bileşimi olan gri kutu olarak isimlendirilen üç farklı test yöntemlerinden oluşur. Kör test olarak da bilinen kara kutu sızma testleri hiçbir arka plan bilgisi ve erişim izni olmadan sıradan bir kullanıcı yetkisiyle yapılır. Beyaz kutu testinde ise, sızma testlerini yapan uzmanlara güvenlik bilgileriyle ilgili önceden gerekli bilgiler verilir. Gri kutu testinde ise testi yapacak uzmanlar bazı alanlarla ilgili bilgi sahibi olurken bazı alanlarda bilgi sahibi olmalarına gerek kalmaz. Bilgi sahibi olunan alanlar, zaman ve bütçe kısıtlarına göre testlere başlamadan önce tanımlanmıştır [3].

Sızma testlerinin yapıldığı lokasyonların seçimi de önemli olup harici ve dâhili olmak üzere iki farklı şekilde yapılabilir. Harici lokasyondan yapılan sızma testlerinde web sitesi ve harici ağ sunucuları gibi dış lokasyondaki teknolojler sınanırken bazı durumlarda, testler uzak bir yerden yürütülür veya test dış lokasyondaki park halindeki bir araçtan yapılabilir. Dâhili lokasyondan yapılan bir testte testler bilişim sistemlerinin yer aldığı iç lokasyonlardan gerçekleştirilir. Bu tür bir test, özellikle görevini kötüye kullanan veya kimlik hırsızlığına maruz kalmış bir çalışanın bilişim sistemine ne kadar zarar verebileceğinin ortaya konulmasında yararlıdır. Bilgi güvenliğinin sağlanmasının bir parçası olarak değerlendirilmesi gereken sızma testleri düzenli aralıklarla veya konfigürasyonlar değiştiğinde tekrarlanmalıdır.

Sızma testleri, yazılım uygulamaları ile otomatikleştirilebilir veya manuel olarak elle gerçekleştirilebilir. Her iki durumda da, testten önce hedef sistem hakkında bilgi toplanması (keşif) ve olası giriş noktalarının belirlenmesi, sızma çalışmaları ve bulguların geri bildirilmesi aşamaları yer alır. Sızma testleri bir kuruluşun güvenlik politikası uygunluğunu test etmek, çalışanların güvenlik bilincini sınamak, bir kuruluşun güvenlik olaylarına cevap verilmesi yeteneğinin test edilmesi ve güvenlik seviyesinin değerlendirilmesi amacıyla birçok ticari veya açık kaynak araçlar kullanılarak yapılır [4].

Sızma testlerinin kolay ve anlaşılır kılınması amacıyla yaygın olarak kullanılan terminolojiler Tablo 12.1'de verilmiştir.

Kitabın bu bölümündü yapılan acıklamaların daha iyi anlaşılması için Tablo 12.1'de kullanılan terminolojiler ve bunların açıklamaları verilmiştir.

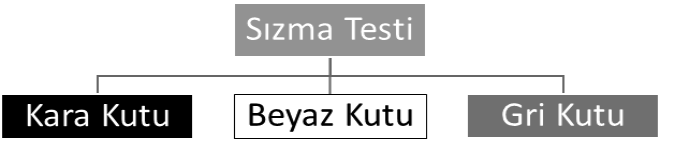
Tablo 12.1. Sızma Testi Terminolojileri

Terminoloji	**Açıklama**
Tehdit (Threat)	Güvenlik ihlaline yol açabilecek potansiyel durum, ortam veya davranış
Zafiyet (Vulnerability)	Sisteme hata yaptırabilecek, istenmeyen bir davranışa sebep olabilecek mantıksal veya üretim hatası
İstismar (Exploit)	Bilgisayar sistemlerinde böcek (bug) veya zafiyet kullanarak yetkisiz erişim, yetki yüseltme, hizmeti devre dışı bırakma (denial of service)
Saldırı (Attack)	Gizliliği ifşa edilmiş olan bilgisayar sistemi güvenlik açıklığının istirmar edilmesidir.

Bu bölümün geri kalan kısımları aşağıdaki şekilde düzenlenmiştir. Bölüm 12.2'de, sızma testlerinin türleri anlatılmıştır. Bölüm 12.3'te sızma testine karşı zafiyet değerlendirmesi tartışılmaktadır. 12.4. bölümde güvenlik testi metodolojileri açıklanmıştır. Bölüm 12.5'de sızma testi aşamaları anlatılmıştır. Bölüm 12.6'da güvenlik testi etiğiden bahsedilerek 12.7. bölümde sonuçlardan bahsedilmiştir.

12.2. Sızma Testi Türleri

Sızma testleri, kara kutu, beyaz kutu ve gri kutu olmak üzere şekilde gerçekleştirilir. Her bir sızma testi türü, kendine özgü özelliklere sahiptir. Sızma testi gerçekleştirilirken amaca yönelik test türünün seçimi, bilişim altyapısının özelliklerine ve elden edilmek istenen çözüm önerilerine göre seçilir. Şekil 12.1'de sızma testi türleri gösterilmiştir. Bu test türleri alt başlıklarda kısaca açıklanmıştır.



Şekil 12.1. Sızma Testi Türleri

12.2.1. Kara Kutu Sızma Testi

Kara kutu sızma testi, gerçek bir saldırıyı tam olarak taklit edebilen sızma test türüdür. Kara kutu testinde, testi gerçekleştiren sistem veya uzmanlar, bilişim sisteminin mimarisi, yazılımı veya donanımı hakkında bilgi sahibi olmazlar. Kara kutu sızma testi, bir saldırgan (black hat hacker) bilişim sistemine nasıl saldırıyorsa, o şekilde planlanır ve gerçekleştirilir [5]. Kara kutu sızma testi, bilişim sisteminde bulunan bütün olası güvenlik açıklıklarını veya zafiyetlerini belirlemek için, hedefleri uygun şekilde tanımlayarak, bütün potansiyel saldırı mekanizmalarını, sistemi tehlikeye atmak için kullanır. Kara kutu sızma testi çok zaman alıcı ve pahalı bir test türüdür. Ayrıca bu testin yapıldığı sistemlerde sistem aksaması ve kalıcı hasarın meydana gelmesi mümkündür. Dolayısıyla sızma testini gerçekleştiren güvenlik uzmanlarının, bilişim sistemlerinde hasara yol açmamak için çok dikkatli olmaları gereklidir. Kara kutu sızma testi sonucunda raporlanan bulgular kurumlar veya müşteriler için kritik öneme sahiptir [6].

12.2.2. Beyaz Kutu Sızma Testi

Beyaz kutu test türünde, sızma testini yapacak güvenlik uzmanı, bilişim sisteminin uygulama, donanım ve yazılım gibi bütün varlıklarını tespit ederek envarterini çıkarır. Bu envanterde bilgisayar ağ topolojisi, işletim sistemi türleri, sistem yama seviyeleri ve uygulamaların kaynak kodları da bulunur. Beyaz kutu testinde, sızma testini yapan uzman, gerçek bir saldırı ile aynı şekilde saldırmayla ilgilenmez, bunun yerine testi yapılması planlanan sistemin güvenlik denetimi ile ilgilenir. Beyaz kutu test türü genellikle yeni geliştirilen uygulamalar için veya bilgisayar ağına yeni eklenen cihazlardan kaynaklanan güvenlik zafiyetlerini tespit etmek için kullanılır. Testi yapan güvenlik uzmanı, teste başlamadan ve gerçek tehditlerine maruz kalmadan önce gelişmekte olan sistemlerdeki güvenlik zafiyetlerini bulmaya çalışır. Bu testler gelişmiş güvenlik programlarında, Sistem Geliştirme Yaşam Döngüsü (Systems Development Life Cycle - SDLC) parçası olarak yürütülür. Sonuç olarak, bu testler

yeni bir uygulama devreye alınmadan ve yeni bir sistem devreye alınmadan güvenlik zafiyetlerini tespit etmek ve bunlara çözüm bulmak için uygun maliyetli bir sızma test türüdür [6,7].

12.2.3. Gri Kutu Sızma Testi

Gri kutu sızma testi, kara ve beyaz kutu testlerinin, karışımı olarak değerlendirilebilir. Gri kutu test türünde, sızma testini gerçekleştiren sistem veya güvenlik uzmanları, değerlendirilmek istenen hedef sistem, uygulama, donanım veya yazılım hakkında bazı bilgilere sahip olurlar. Bu bilgiler, işletim sistemi sürümleri veya bilgisayar ağ mimarisi ile ilgili sınırlı olabilir. Kara kutu sızma testinde olduğu gibi bilişim sistemi ile ilgili hiçbir şey bilmeden veya beyaz kutu sızma testinde olduğu gibi bilişim sistem ile ilgili olarak her şeyi bildikleri varsayılmaz. Gri kutu sızma testleri, kurumlar tarafından talep edilen, belirli bir güvenlik zafiyetini test etmek için kullanılır. Yani, bilişim sistemlerinde, belirli bir bölgenin veya işlemin güvenlik testini yapmak için kullanılır. Örneğin; bilişim ağında, eposta sunucusu katmanını test etmek için sızma testi gerçekleştirilebilir. Bu durumda, sızma testini gerçekleştiren güvenlik uzmanı, testi yapılacak sınırlı alanın IP adres katmanları ve bağlı olan diğer sistemlerin özel bilgilerine sahip olabilir. Gri kutu sızma testinde, bilişim sistemi bileşenlerinin güvenlik zafiyet denetimleri çevrimiçi olarak gerçekleştirilir [6,7].

12.2.4. Sızma Testine Karar Verme

Bir bilişim sistemine hangi sızma testinin uygulanacağına, sızma testini yapan güvenlik uzmanı ve kurumun ihtiyaçları doğrultusunda kurumun kendisi karar verir. Örneğin; eğer sistemleri test edilecek kurum yeni bir sistemi geliştirme aşamasından üretim aşamasına taşıyor ve güvenlik ayarlarının doğru şekilde yapıldığından emin olmak istiyorsa, genellikle beyaz kutu sızma testine karar verilir. Öte yandan, gelişmiş bir güvenlik stratejisi olan ve bütün güvenlik sistemini gerçek saldırılar açısından test ettirmek isteyen bir kurum için ise kara kutu sızma testi kullanılacaktır. Ayrıca sızma testinin yapılacağı, hedef kurumun sızma test tecrübesi dikkate alınmalıdır. Sızma testleri için yeni olan kurumlar, bilişim sistemlerinin zarar göreceğinin olumsuz etkileneceği düşünülerek, sızma testinin ger-

çekleştirilmesinde tereddütler yaşarlar. Genelde, beyaz kutu sızma testi, kurumların bu tereddütlerinin ortadan kaldırılması bakımından önemli bir çözümdür [2,3].

12.3. Sızma Testine Karşı Zafiyet Değerlendirmesi

Güvenlik zafiyeti değerlendirmesini doğru bir şekilde anlamaya ve uygulamaya her zaman ihtiyaç vardır. Kurumların bilişim sistemleri için, bir değerlendirme türü belirlemeye karar verirken sızma testi kavramını yanlış yorumlayan ticari ve ticari olmayan kurumlarla karşılaşılabilir. Dolayısıyla sızma test türleri arasındaki farkları bilmek çok önemlidir. [3] Güvenlik zafiyeti değerlendirmesi, kurumsal varlıklar için ciddi risk oluşturan tehditleri belirleyerek iç ve dış güvenlik denetimlerini değerlendiren bir süreçtir. Teknik altyapı değerlendirmesi, sadece var olan savunma sistemindeki riskleri ortaya çıkarmakla kalmayıp aynı zamanda, çözüm stratejilerini de önceliklendirerek tavsiye raporu oluşturmalıdır. Kurum içi güvenlik zafiyeti değerlendirmesi dâhili sistemlerin güvenliği için güvence sağlarken, kurum dışı güvenlik zafiyeti değerlendirmesi hem kurum içi hem de çevre korumasının güvenliğinin risk seviyesini gösterir. Her iki sızma testi türünde, bilgisayar ağındaki her bir varlık, henüz meydana gelmemiş tehditleri ve reaktif önlemleri belirlemek için çoklu saldırılara karşı titizlikle test edilmelidir. Gerçekleştirilen güvenlik zafiyet değerlendirme türüne bağlı olarak, bilgi varlıklarındaki güvenlik zafiyetlerini otomatik olarak tespit etmek ve tanımlamak için bir dizi test etme süreci, araç ve teknikler takip edilir. Bu sadece, yapılandırma ve değişiklik yönetiminin bütünlüğünü korurken, güncel güvenlik zafiyeti veritabanı yöneten ve bilgisayar ağ cihazlarının farklı türlerini test edebilen entegre güvenlik zafiyeti yönetme platformu kullanılarak gerçekleştirilebilir [8].

Güvenlik zafiyeti değerlendirmesi ile sızma testi arasındaki temel fark, sızma testinin güvenlik zafiyetlerini belirlemenin de ötesinde, sömürü süreci, ayrıcalık tanımlama ve hedef sistemlere erişimin sürdürülmesini sağlamasıdır. Öte yandan güvenlik zafiyeti değerlendirmesi, sistemdeki hataları tespit eder ama, bu hataların söz konusu bilişim sistemine olan maliyet etkisini dikkate almaz. Bu iki kavram arasındaki diğer önemli fark, sızma testinin güvenlik zafiyeti değerlendirmesinden daha müdahaleci olması ve bilişim sisteminde bütün teknik metotları saldırgan bir şekilde kullanır. Fakat

güvenlik zafiyeti değerlendirmesi süreci bütün bilinen güvenlik zafiyetlerini inovatif olarak dikkatlice belirler ve ölçer. Değerlendirme türlerinin birlikte ele alınması, terimlerin birbirleri ile karıştırılmasına sebep olabilir. Nitelikli bir güvenlik uzmanı, kurumların iş ihtiyaçlarına göre en iyi değerlendirme türünün seçilmesinde yardımcı olur. Ayrıca son kararı vermeden önce seçilen güvenlik değerlendirme programının temel ayrıntılarını incelemek sözleşmeyi yapan tarafın sorumluluğundadır [9].

12.4. Güvenlik Testi Metodolojileri

Güvenlik zafiyetlerini değerlendirmek için birçok açık kaynak metodoloji vardır. Bilişim sistemi ne kadar büyük veya karmaşık olursa olsun, zafiyet değerlendirme metodolojileri kullanılarak sistem güvenliği sağlanabilir. Bazı metodolojiler güvenlik testinin teknik tarafına odaklanırken, bazıları da sadece yönetimsel kriterlere odaklanmaktadır. Bu güvenlik testi metodolojilerini kullanmanın amacı, bir sistemin güvenlik zafiyetlerini doğru bir şekilde değerlendirmektir [10,11].

Bazı güvenlik metodolojileri aşağıda verilmiştir;

- Açık Kaynak Güvenlik Test Metodolojisi Kılavuzu (Open Source Security Testing Methodology Manual - OSSTMM)
- Bilgi Sistemleri Güvenlik Testi Çerçevesi (Information Systems Security Assessment Framework - ISSAF)
- Açık Web Uygulama Güvenliği Proje Test Kılavuzu (Open Web Application Security Project Testing Guide - OWASPTG)
- Web Uygulama Güvenliği Konsorsiyum Tehdit Sınıflaması (Web Application Security Consortium Threat Classification - WASCTC)
- Sızma Testi Yürütme Standardı (Penetration Testing Execution Standard - PTES)

Sızma testi yöntemleri, güvenlik uzmanlarına, kurumların güvenlik gereksinimlerine uygun en iyi test stratejisini seçme konusunda yardımcı olurlar. OSSTMM ve ISSAF yöntemleri, hemen hemen bütün kurumsal bilgi varlıklarına yönelik kurallar ve güvenlik testi

politikaları sunmaktadır. OWASPTG ve WASCTC tarafından sunulan sızma testi kılavuzu, bir uygulamanın güvenlik zafiyetlerini belirlemek için çözüm üretir. PTES ise her türlü sızma testi girişimi konusunda rehberlik yapabilir. Güvenlik kendi içinde bir süreçtir ve sızma testleri, bilişim sistemlerinin güvenlik zafiyetleri ile ilgili önemli çözümler üretir. Sızma testi sırasında bilişim sistemlerinde yapılacak bir küçük değişiklik, güvenlik test sürecinin tamamını etkiler ve sonuçlarda hatalara sebep olabilir. Tek bir sızma testi yöntemi kullanmak, güvenlik risk değerlendirmesi konusunda yeteri kadar detaylı bir çözüm önerisi sunmaz. En iyi sızma testi yönteminin seçimi, hedef kurumun özelliklerine göre ve sızma testini gerçekleştirecek uzmanların görüşlerine göre yapılmalıdır [2,3,4,12].

Birçok güvenlik test metodolojisi arasından, maliyet ve etkililik bakımından en iyisini seçmek için, dikkatli bir seçim sürecine ihtiyaç vardır. Doğru bir sızma test yöntemi seçimi, hedef ortam, kaynak kullanılabilirliği, güvenlik uzmanı bilgisi, iş hedefleri, bilişim sistemi teknik detayları gibi çeşitli faktörlere bağlıdır.

12.5. Sızma Testi Aşamaları

Sızma testi için kullanılan donanım veya yazılımlar, güvenlik değerlendirmesi ve sızma testi araçlarıyla birlikte sunulan çok yönlü işletim sistemlerine sahip olmalıdırlar. Bu sistemlerin altyapıdan yoksun olması ve uygulanması başarısız sızma testlerine yol açabilir ve hatalı raporlamanın yapılmasına sebep olabilir. Başarılı bir sızma testinin gerçekleştirilmesi ve doğru raporlama yapılması için, gerekli planlama ve altyapıya sahip sistemlerin kullanılması, güvenlik testinin teknik perspektifi açısından çok önemlidir [3,4].

Burada sunulan sızma testi yapısı, hem kara kutu hem de beyaz kutu sızma testi yaklaşımlarından oluşmaktadır. Sızma testi öncesinde, güvenlik uzmanının veya test sisteminin yapması gereken aşamalar için genel bir yaklaşım sunulmuştur. Bu yaklaşımlar, değerlendirme hedeflerine göre düzenlenebilir. Sızma testinin başarılı bir şekilde yapılması için başlangıç, orta ve son aşamasında bazı süreçlerin adım adım takip edilmesi gereklidir.

Bu süreçler maddeler halinde aşağıda verilmiştir.

(1) Hedefin Kapsamını Belirleme

(2) Hedef Hakkında Bilgi Toplama
(3) Hedefi Keşfetme
(4) Hedefin Envanterini Belirleme
(5) Güvenlik Açığı Eşlemesi
(6) Sosyal Mühendislik
(7) Hedefi İstismar Etme
(8) Yetki Yükseltme
(9) Erişimi Sağlamak
(10) Dokümantasyon ve Raporlama

Sızma testi adımlarının tamamının ve bir kısmının kullanılması hedef alınacak sisteme ve yapılacak sızma testi türüne (Kara Liste, Beyaz Liste, Gri Liste) göre farklılık gösterebilir. Bu yaklaşımlar, var olan yöntemlerden biri ile birleştirilerek, güvenlik uzmanları tarafından yol haritası olarak kullanılabilir [3].

12.5.1. Hedefin Kapsamını Belirleme (Target scoping)

Bir güvenlik zafiyet değerlendirmesine başlamadan önce; sızma testi yapılacak hedef bilişim ağının incelenerek, kapsamı hakkında bilgi sahibi olunması çok önemlidir. Ayrıca sızma testini gerçekleştirecek güvenlik uzmanının, testin yapılacağı ağın kapsamını ve testin sınırlarını bilmesi gereklidir. Hedefin kapsamını belirlemek için cevaplandırılması gerekenler sorular halinde aşağıda verilmiştir:

- Ne test edilecek?
- Nasıl test edilecek?
- Test sürecinde hangi koşullar uygulanacak?
- Testin sınırları nelerdir?
- Test ne kadar sürede tamamlanacak?
- Test sonunda hangi başarılar sağlanacak?

Güvenlik uzmanı, başarılı bir sızma testi için, test edilecek hedef sistemin işlevinin ve ağ ortamıyla etkileşimlerinin farkında olmalıdır. Çünkü güvenlik uzmanın hedef sistem ile ilgili bilgisi, sızma testinin başarısına önemli katkı sağlayacaktır [3,12].

12.5.2. Hedef Hakkında Bilgi Toplama (Information gathering)

Sızma testi için hedef bilişim sistemi kapsamı öğrenildikten sonra, hedef ile ilgili bilgi toplama aşamasına geçilebilir. Bu aşamada, sızma testini gerçekleştirecek uzman hedef ile ilgili özellikle kamuya açık kaynakları araştırarak bilgi elde edebilir.

Bilgi elde edilebilecek kaynaklar aşağıda maddeler halinde verilmiştir. gibi internet tabanlı uygulamalar olabilir.

- Forumlar
- E-posta veya bülten grupları
- Makaleler
- Bloglar
- İnternet tabanlı uygulamalar
- Sosyal ağlar
- Ticari veya ticari olmayan web siteleri vb.

Kurum hakkındaki bilgiler arama motorları kullanılarak da toplanabilir. Güvenlik uzman, hedefe ait ağ bilgilerini elde etmek için sızma testi için kullandığı sistemin işletim sistemi araçlarını kullanabilir. Bu araçlar, veri madenciliği yöntemlerini kullanarak DNS sunucuları, who.is veritabanı, e-posta adresleri, telefon numaraları, kişisel veriler ve kullanıcı hesaplarını bulabilirler. Ne kadar fazla bilgi toplanırsa, daha başarılı sızma testi yapma olasılığı artar. Hedef sistemlerle ilgili daha fazla bilgi toplamak için derin web de kullanılabilir. Sadece TOR tarayıcısı ile erişilebilen derin web, istismarlarla ilgili bilgi ve test edilen kuruluştan elde edilen bilgileri bulundurabilir [3, 13].

12.5.3. Hedefi Keşfetme (Target discovery)

Hedef bilişim ağ altyapısı, işletim sistemi ve ilgili bilgisayar ağının mimarisi tanımlanır. Ağ altyapısını oluşturan teknolojilerin veya cihazların özellikleri belirlenir ve ağ üzerinde çalışan çeşitli hizmetlerin envanteri oluşturulur. Örneğin, sızma testlerinde en çok kullanılan işletim sistemlerinden olan, Kali Linux ağ cihazlarını kullanarak, ana (omurga) cihazlarda çalışan bilgisayar ağı ana bilgisayarlarını ve işletim sistemlerini belirleyebilir ve her cihazı ağ içindeki rolüne göre gruplayabilir. Bu araçlar genellikle aktif veya pasif denetim ya-

pabilmek için bilişim ağının önüne konumlandırılır [3,14].

12.5.4. Hedefin Envanterini Belirme (Enumerating target)

Bu aşama, daha önce yapılan çalışmalara katkı sağlayarak hedef sistemlerde bulunan açık portların tespit edilmesini sağlar. Açık portlar belirlendikten sonra, veri paylaşımı için kullanılan servislerin envanteri çıkarılır. Hedef ana bilgisayar veya sistem bir güvenlik duvarı veya saldırı tespit sisteminin (IDS) arkasında olsa bile, açık, yarı açık veya gizli port tarama teknikleri kullanılarak, portların istismar edilmesini veya ortaya çıkarılmasını sağlayabilir. Belirlenen portlar ile eşleşen servisler veya hizmetler, hedef bilgisayar ağının altyapısında bulunan güvenlik açıklarının ortaya çıkarılmasını sağlar. Aslında bu aşamanın görevi, ağ cihazlarındaki güvenlik açıklarını bularak, sızma testini başarılı bir şekilde gerçekleştirmektir [3, 15].

12.5.5. Güvenlik Açığı Eşlemesi (Vulnerability mapping)

Bir önceki aşamaya kadar, hedef bilgisayar ağı hakkında yeterli bilgi toplandı. Artık tespit edilen port ve servisler kullanılarak güvenlik zafiyetleri belirlenebilir ve analiz edilebilir. Bu süreç, sızma testi için kullanılan işletim sisteminde bulunan ağ ve uygulama güvenlik zafiyeti değerlendirme araçları kullanılarak otomatik olarak yapılabilir. Bu işlem manuel olarak da yapılabilir ancak çok fazla zaman alır ve güvenlik uzmanı bilgisine ihtiyaç duyulur. Bununla birlikte, her iki yaklaşım birleştirilerek, bilgisayar ağlarında veya uygulamalarda bulunan bilinen veya bilinmeyen güvenlik zafiyetini tespit etmek için deneyimli bir güvenlik uzmanına ihtiyaç vardır [3, 16].

12.5.6. Sosyal Mühendislik (Social engineering)

Bir güvenlik uzmanı, hedef bilgisayar ağına girmek için açık kapı bulamadığı zaman, sosyal mühendisliği deneyebilir. Sosyal mühendislik ile insan faktörü kullanılarak bir yetkili veya bir kullanıcı kandırılabilir, arka kapı erişimini sağlayan kötü amaçlı kod ele geçirilerek, hedef sisteme sızmak mümkün olabilir. Sosyal mühendislik farklı formlarda uygulanabilir. Örneğin; telefonda bilgisayar ağı yöneticisi gibi davranan, hesap bilgilerini paylaşması için zorlayan veya banka hesap bilgilerini ele geçirmek için e-posta ile sazan avlama yöntemleri kullanılarak kimlik bilgilerinin talep edilmesi

şeklinde olabilir. Fiziksel bir ortama girmek için kurum personeli taklidi yapan birisinin davranışı da sosyal mühendislik olarak düşünülebilir. Sosyal mühendislikte, istenilen amaca erişmek için, uygulanacak oldukça fazla sorumluluk kümesi veya davranış şekli vardır. Başarılı bir sızma testi için, hedefe karşı herhangi bir aldatma uygulamadan önce insan psikolojisini anlamak için gerekli zamana ihtiyaç duyulabilir. Ayrıca bu aşamaya gelmeden önce sosyal mühendislikle ilgili yasaların iyi bilinmesi önemlidir. Çünkü sosyal mühendislik yasal olarak cezai hükümler içeren davranış türüdür [3,17,18].

12.5.7. Hedefi İstismar Etme (Target exploitation)

Ortaya çıkarılan güvenlik zafiyetleri dikkatlice incelendikten sonra, yapılabilecek istismar çeşitleri kullanılarak, hedef sisteme sızmak mümkündür. Bazen, tespit edilen zafiyeti başarılı şekilde istirmar etmek için, ek araştırma yapmak veya mevcut istismarı düzenlemek gerekebilir. Ayrıca, güvenlik uzmanı hedef bilişim sistemini kontrol altında tutmak için, sosyal mühendislik ile karışık müşteri taraflı istismar yöntemlerini uygulayabilir. Bu yüzden, bu aşamada zaten hedef sistemin zafiyetleri tespit edilmiş ve artık zafiyetler ve istismar yöntemleri kullanılarak, hedef sistemde sürekli olarak erişimi canlı tutmaktadır. İstismar süreci, istismar öncesi, istismar sırası ve istismar sonrası olmak üzere üç aşamada koordine edilir [3,19].

12.5.8. Yetki Yükseltmek (Privilege escalation)

Hedef ele geçirildiğinde, sızma testi başarılı şekil gerçekleştirilmiş demektir. Güvenlik uzmanı erişim yetkisine bağlı olarak sistem içinde serbestçe hareket edebilir. Sızma testi ile elde edilen yetki, süper kullanıcı yetkisi olabilir veya sistemde farklı kullanım ayrıcalıklarına izin verebilir. Bu da erişimi sağlanan hedef sistemin yeterince kötüye kullanılmasına sebep olabilir. Güvenlik uzmanı bu erişim yetkisini kullanarak, yerel bilgisayar ağında daha fazla saldırı başlatabilir. Bu süreç verilen hedefin kapsamına bağlı olarak sınırlandırılabilir ya da sınırlandırılamayabilir. Ağ trafiğini dinleyerek çeşitli servislerin parolalarını çözerek ve yerel ağ aldatma (spoofing) yöntemlerini uygulayarak, ele geçirilen hedefte daha da fazla yetki yükseltmesi yapılabilir. Sonuçta, yetki yükseltme amacı sisteme mümkün olan en yüksek seviye girişini kazanmaktır [3, 20].

12.5.9. Erişim Sağlamak (Maintaining Access)

Sızma testini gerçekleştiren güvenlik uzmanından belirli bir süre için sisteme erişmesi istenebilir. Bu faaliyet, sızma testi sürecini gerçekleştirmeden bilişim sistemine illegal erişimi kanıtlamak için kullanılabilir. Böylece sızma testi sürecinde harcanan zaman, maliyet ve kaynaklardan tasarruf sağlanabilir. Arka kapı erişimini sağlayan protokol, proxy veya uçtan uca bağlantılardan yararlanan gizli tünelleme yöntemleri, güvenlik uzmanının izlerini hedef sisteme eklemesine yardımcı olur. Bu tür sistem erişimleri, bir saldırganın sistemde, kendini belli ettirecek işlemler yapmadığı takdirde sürekli var olmasını sağlar [3, 21].

12.5.10. Belgeleme ve Raporlama (Documentation and reporting)

Tespit edilen ve istismar edilen güvenlik açıklarını belgelemek ve raporlamak, sızma testinin tamamlanma aşamasıdır. Belgelendirme ve raporlama etik açıdan çok önemlidir, çünkü yönetim, sızma testi ekibini denetleyebilir ve bulunan güvenlik zafiyetlerini kapatmak yeni bir iş süreci başlatabilir. Sızma testi sonucunda, kurumlar için oluşturulan raporlar, bilişim altyapısında var olan zayıf noktaları anlama ve analiz etme konusunda teknik personele yardımcı olacaktır. Ayrıca, belgeler ve raporlar, sızma testinden önce ve sonra hedef bilişim sisteminin güvenlik açısından karşılaştırılmasına imkan sağlamalıdır [2,3,22].

12.6. Güvenlik Testi Etiği

Güvenlik testinin etik değeri, sızma testini yapacak güvenlik uzmanı tarafından profesyonel, etik ve yetkili uygulamaları ile ilgili takip edilmesi gereken sözleşme kurallarından oluşur. Etik kurallar, sızma testi hizmetlerinin nasıl sunulacağını, testin nasıl gerçekleştirileceğini, yasal sözleşmeleri ve görüşmelerin nasıl belirlendiğini, testin kapsamını tanımlamayı, test planını hazırlamayı, test sürecini izlemeyi ve tutarlı bir raporlamanın nasıl hazırlanacağından oluşur. Bu alanların tamamına uymak, dikkatli bir inceleme gerektirir ve test boyunca resmi uygulama ve prosedürler de takip edilmelidir [3,12,23].

Bu kuralların bazı örnekleri aşağıdaki gibi tartışılmıştır:

- Kurum (müşteri) ile güvenlik uzmanı arasında herhangi bir resmi anlaşma yapılmadan hedef sisteme girerek test yapılmamalı-

dır. Bu etik olmayan bir pazarlama yöntemidir, çünkü böyle bir iş başarısızlıkla sonuçlanabilir ve yetki alanlarına bağlı olarak ciddi yasal çıkarımlara neden olabilir.

- Test kapsamı dışında bir test yapılması ve müşteriden izin alınmadan belirlenen test sınırlarının dışına çıkılması yasaktır.
- Sözleşmede, tarafların sorumlulukları, test şartları ve koşulları, acil durum iletişim bilgileri ve çalışma beyanı herhangi bir çıkar çatışmasına izin vermeden açıkça belirtilmelidir.
- Test planı, sızma test süresini çalışma zamanlarını içermelidir. Kurumun iş saatlerini ve üretimini kesintiye uğratmayacak şekilde planlanmalıdır.
- Test süreci, sızma testi sırasında takip edilmesi gereken kuralları ifade eder.
- Kapsam tanımı, sözleşme taraflarını ve güvenlik değerlendirmesi sırasında uygulanan sınırları açıkça tanımlamalıdır.
- Güvenlik test sonuçları, belgelenerek ve raporlanarak net, tutarlı ve doğru bir şekilde sunulmalıdır. Raporlar bilinen ve bilinmeyen tüm güvenlik zafiyetlerini açıklamalıdır. Sonuç raporu sadece kurum yetkilisine teslim edilmelidir.

12.7. Değerlendirmeler

Sızma testleri bilişim sistemlerinin güvenliğine etki eden iç ve dış faktörlerin bir bütün olarak saldırgan gözüyle sınanmasıdır. Bilişim sistemlerinin güvenlik zafiyetlerinin tespit edilerek giderilmesi için yapılacak düzeltmelerin belirlenmesi, sızma testlerinin bilişim sistemlerinin güvenliğinin sağlanmasında önemli bir süreçtir. Yüksek seviyede bilgi güvenliğinin sağlanmasında sızma testleri yaşayan bilişim sisteminin güvenliği merkezinde yer alır ve bilgi güvenliğinin devamlılığının sağlanmasında önemli rol oynar.

Sızma testleri, bilişim sistemlerinin olumsuz bir durum ile karşılaşılmadan önce, bilişim sistemi açıklarını önleyecek ve alınabilecek karşı tedbirlerin düşünülmesinde kullanılan önemli bir erken uyarı sistemidir. Sızma testlerinin başarılı olabilmesi için kurumların güvenliğine etki eden faktörlerin ağırlıkları dikkate alınarak kuruma özgü farklı senaryolar geliştirilmesi gereklidir. Sızma testleri için geliştirilen senaryolar kurumlarda kullanılan teknolojilere, çalışan-

ların bilgi düzeylerine, bilgi güvenliği seviyesine, bilgi güvenliği bileşenlerine göre farklılık gösterebilir.

Sızma testleri, bilişim sistemleri ihlallerinin kontrollü bir şekilde tespit edildiği, kurumsal bilgi güvenliğinin sağlanması için düzenli olarak yapılan ve proaktif önlemler alınmasını sağlayan bilişim sistemi güvenliği yöntemleridir. Sızma testlerinin başarısı gerçek dünyada bilgi güvenliği için tehditler oluşturan saldırganların teknik ve taktiklerinin tam olarak simülasyonuna bağlıdır. Düzenli olarak yapılan sızma testleri, kurumların bilgi güvenliği zafiyetlerinin ve ihtiyaçlarının çıkartılarak siber saldırılara karşı önlem alınmasını sağlar.

Oldukça maliyetli bilişim sistemleri üzerinde yapılacak sızma testleri sonucunda zafiyetlerin tespit edilerek bilişim sistemlerinin güvenlik açıklarının giderilmesi zaman ve maliyet açısından uygun ve istenen bir çözümdür.

Sonuç olarak sızma testi yöntemleri anlatılarak sızma testi terminolojileri açıklanmıştır. Sızma testlerinin özellikleri aşağıdaki gibi özetlenebilir.

- Sızma testi, kara kutu ve beyaz kutu ve gri kutu gibi farklı türlerden oluşur. Kara kutu yaklaşımı, test uzmanının, hedef sistem hakkında önceden bilgisinin olmadığı, harici bir test türüdür. Beyaz kutu yaklaşımı ise, test uzmanını hedef ortamı bildiği ve kurum içi testlere atıfta bulunduğu bir yaklaşımdır. Kara kutu ve beyaz kutu türlerinin kombinasyonu ise gri kutu yaklaşımıdır.
- Bilişim sistemlerinde güvenlik açığı değerlendirmesi ve sızma testi arasındaki önemli fark, güvenlik açığı değerlendirmesi sistemde var olan hataların zafiyet etkisini veya maliyetini bilinmeden açıklığın tespit edilmesidir. Sızma testleri ise bilişim sistemlerinde var olan hataların veya zafiyetlerin maliyet etkisini de ölçebilir ve sonuçlarını değerlendirebilir.
- Birçok güvenlik testi yöntemi vardır, ancak bunlardan sadece bazıları bilişim sisteminin veya uygulamanın güvenlik seviyesini ölçmek için, yeterli olgunluğa sahiptir. Teknik yetenekleri ve temel özellikleri bakımından OSSTMM, ISSAF, OWASP, PTES ve WASC-TC açık kaynaklı güvenlik değerlendirme metodolojileridir.

- Sızma testi süreci, güvenlik testine yönelik organize edilen bir dizi adımdan oluşmaktadır. Bunlar arasında hedef kapsam belirleme, bilgi toplama, hedef bulma, hedef belirleme, güvenlik açığı eşlemesi, sosyal mühendislik, hedef sömürü, ayrıcalık yükseltme, erişimi sürdürme ve belgeleme ve raporlama adımları yer almaktadır.
- Güvenlik değerlendirme sürecinin gerçekleştirilebilmesi için uyulması gereken sızma testi etik değerleri araştırılmıştır. Güvenlik zafiyet değerlendirme çalışmasının her adımında etik değerlere uyulması, güvenlik uzmanı ve kurum arasında bu süreç başarılı bir şekilde yürütülmelidir [2,3,8,9,22].

Kaynaklar

[1] Vacca, J. R. (Ed.)., Managing information security. Elsevier, 2013.

[2] Y. Vural, "Kurumsal Bilgi Güvenliği ve Sızma Testleri", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 40, 2007.

[3] Johansen, G., Allen, L., Heriyanto, T., & Ali, S., Kali Linux 2-Assuring Security by Penetration Testing. Packt Publishing Ltd, 2016.

[4] Whitaker, A., & Newman, D. P., Penetration testing and network defense. Cisco Press, 2005.

[5] Muniz, J., Web Penetration Testing with Kali Linux. Packt Publishing Ltd., 2013.

[6] Khan, M. E., & Khan, F., A comparative study of white box, black box and grey box testing techniques. Int. J. Adv. Comput. Sci. Appl, 3(6), 2012.

[7] Caselli, M., Kargl, F., & Limmer, T. D5. 1 Security Testing Methodology.

[8] Broder, J. F., & Tucker, E., Risk analysis and the security survey. Elsevier, 2011.

[9] Geer, D., & Harthorne, J., 2002, Penetration testing: A duet. In null (p. 185). IEEE, 2002.

[10] Robinson, M., Jones, K., Janicke, H., & Maglaras, L., Developing Cyber Peacekeeping: Observation, Monitoring and Reporting. arXiv preprint arXiv:1806.02608., 2018.

[11] Thomas, T. W., Tabassum, M., Chu, B., & Lipford, H. Security During Application Development: an Application Security Expert Perspective. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (p. 262). ACM., 2018.

[12] McDermott, J. P., Attack net penetration testing. In Proceedings of the 2000 workshop on New security paradigms (pp. 15-21). ACM., 2001.

[13] Halfond, W. G., Choudhary, S. R., & Orso, A., Penetration testing with improved input vector identification. In Software Testing Verification and Validation, 2009. ICST'09. International Conference on (pp. 346-355). IEEE, 2009.

[14] Halfond, W. G., Choudhary, S. R., & Orso, A., Improving penetration testing through static and dynamic analysis. Software Testing, Verification and Reliability, 21(3), 195-214, 2011.

[15] McLaughlin, S., Podkuiko, D., Miadzvezhanka, S., Delozier, A., & McDaniel, P., Multi-vendor penetration testing in the advanced metering infrastructure. In Proceedings of the 26th Annual Computer Security Applications Conference (pp. 107-116). ACM, 2010

[16] Gleichauf, R. E., Randall, W. A., Teal, D. M., Waddell, S. V., & Ziese, K. J. U.S. Patent No. 6,301,668. Washington, DC: U.S. Patent and Trademark Office, 2001.

[17] Ceraolo, J. P., Penetration testing through social engineering. Information systems security, 4(4), 37-48., 1996.

[18] Dimkov, T., Van Cleeff, A., Pieters, W., & Hartel, P., Two methodologies for physical penetration testing using social engineering. In Proceedings of the 26th annual computer security applications conference (pp. 399-408). ACM, 2010.

[19] Kennedy, D., O'gorman, J., Kearns, D., & Aharoni, M. Metasploit: the penetration tester's guide. No Starch Press, 2011.

[20] Davi, L., Dmitrienko, A., Sadeghi, A. R., & Winandy, Privilege escalation attacks on android. In international conference on Information security (pp. 346-360). Springer, Berlin, Heidelberg.

[21] Engebretson, P. (2013). The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier, 2010.

[22] Hudic, A., Zechner, L., Islam, S., Krieg, C., Weippl, E. R., Winkler, S., & Hable, R., Towards a unified penetration testing taxonomy. In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom) (pp. 811-812). IEEE, 2012.

[23] Whitaker, A., & Newman, D. P., Penetration testing and network defense. Cisco Press, 2005.

Elektrik Enerjisi Sektöründe Siber Güvenlik

BÖLÜM 13

Dr. Mehmet Rıda TÜR
Prof. Dr. Ramazan BAYINDIR - Seyfettin VADİ

ELEKTRİK ENERJİSİ SEKTÖRÜNDE SİBER GÜVENLİK

Bu bölüm, genel olarak gelişen şebeke modeline karşı oluşan siber tehditleri tarif etmektedir. Daha sonra enerji sektörü, güç sistemleri bileşenleri ve siber güvenlik risklerine yönelik genel bir bakış sunmakla beraber üretim santrallerinde kumanda ve güvenlik devresi sistemleri ele almaktadır. Son olarak, siber saldırılar ve alınması gereken önlemler gözden geçirilerek sunulmuştur.

13.1. Giriş

Elektrik şebekelerinin altyapısı modernleştikçe, güç sistemleri her geçen gün daha güncel bir teknolojiyi benimsemek zorunda kalmaktadır. Ancak, enerji sağlayıcılarının önceliği, güvenliğin ötesinde, güvenli bir şekilde elektrik enerjisinin sağlanmasıdır. Yirminci yüzyılın başlarından bu yana, güç sistemleri, elektrik üretiminde ve tüketimde yaşanan büyük orandaki artışlara ayak uydurmak ve aynı şekilde insan gücü ihtiyacını azaltmak için otomasyon sistemlerine giderek daha fazla güvenmektedir.

Güç sistemleri, en yüksek düzeyde güvenilirlik sağlamak için artan sistem koruma, otomasyon ve kontrol kabiliyetlerini sürekli olarak benimsemiştir. Böylece güvenilirlik seviyeleri ve enerji verimliliği arttıkça, gerçek zamanlı bilgi talebi ve güvenilirlik beklentisi de artmaktadır. Bu ilerleyen teknolojik gereksinimleri veri ihtiyaçları ve sistem gereksinimleri, daha geniş otomasyon ve kontrol yeteneklerini kullanmak için sistemlerin modernize olmasını zorlamaya devam etmiştir.

Güç sistemlerinin günlük operasyonları yönetmek için kullandığı bileşenler, şebeke verimliliği için, bölgesel yüklere hizmet etmek için bölgesel üretim santrallerinden yararlanan entegre yardımcı programlarla ve gerektiğinde birimler arası destek için tasarlanmış-

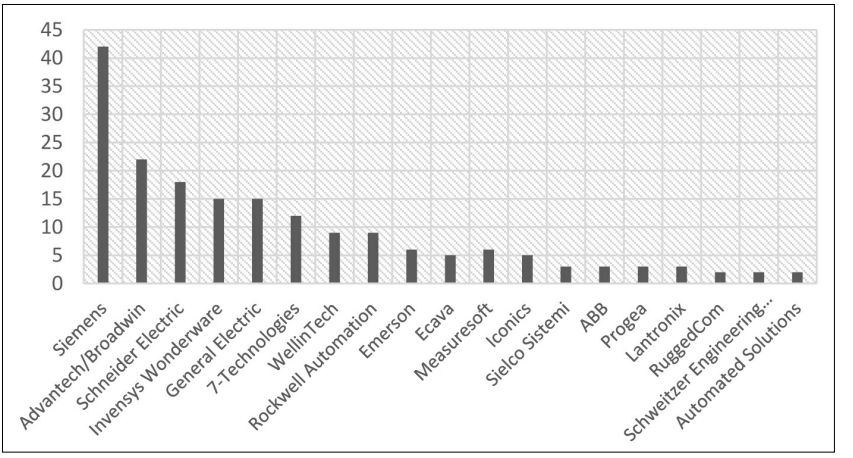
tı. Günümüzün elektrik sistemi, gelişmiş bir iletim sistemine, piyasa operasyonlarına, bağımsız güç üreticilerine, sistem operatörlerine ve genel sistem güvenilirliğini sağlamak için geleneksel olarak bütünleştirilmiş yardımcı programlara dayanmaktadır. Güç sisteminin mühendisliği ve sistemin nasıl işletildiği çok dinamik bir ortamdır. Fakat yeni otomasyon ve kontrol elemanlarının çoğunda, sistemlerin aktif olarak çalıştırıldığı sırada siber tehditlerin potansiyeli fark edilmedi. Güç sistemleri, günümüz ihtiyaçlarını karşılamak için Endüstriyel Kontrol Sistemleri (EKS) ve elektrik şebekesi teknolojisini yükselttikçe, dijital otomasyon ve veri aktarımının daha sık kullanımı gerekli hale gelmiştir. Özellikle gelişmiş iletişim araçları ve İnternet bağlantısı sonucunda daha fazla erişilebilirlik ile ilgili çeşitli zayıflıklar ortaya çıkmıştır

13.2. Gelişen Elektrik Şebekesinde Oluşan Tehditler

Geçmiş dönemlerde Ulusal güç sistemimizde elektrik dağıtımı görevi TEDAŞ tarafından yürütülmekteydi, fakat 2013 yılından itibaren elektrik dağıtım işlemi yirmi bir farklı bölgeye ayrılmış şekilde özel sektöre devredilerek hizmet sunulmaktadır. Bu geçiş süreci ile beraber dağıtım şirketleri şebeke altyapısını güncelleyerek yeni teknolojiler ile sistemi kontrol etmeye başlamıştır. Bu kontrol hizmetlerinin temelinde akıllı şebeke bileşenleri bulunmaktadır. Ayrıca, SCADA otomasyon sistemleri vasıtasıyla uzaktan denetimler yapılmaktadır. Dağıtım şirketleri akıllı sayaç kullanmak suretiyle, elektrik sayaçlarında otomatik okuma sistemleri kullanılmaya başlanmıştır. Fakat gelişen şebeke altyapısı ile paralel ilerlemesi gereken haberleşme koruma ve güvenlik sistemleri güncellememiştir. Bu durum mevcut şebeke altyapısının siber saldırılara karşı daha korunaksız hale gelmesine neden olmakla beraber siber güvenlik önlemleri enerjide arz güvenliği bakımından ciddi bir gereksinim haline gelmiştir.

Siber güvenlik teknolojisinde ve pazarında ilk sıralarda olan ülkeler aynı zamanda da enerji otomasyonu ve teknolojilerinde de benzer durumdadır. Bu piyasa, dünya çapında birçok firma ile yürütülmesine rağmen bazı bölgelerde belirli firmaların tekelinde yürütülmektedir. Siber güvenlik konusunda yapılan son inceleme analizlerinde, haberleşme ağına bağlanmış EKS'nin yaklaşık yüzde 40'ının rahatlıkla kontrol altına alınarak çökertilebileceği ifade

edilerek korumasız oldukları ve genel olarak bu durumu en çok yaşayan şirketlerim dağılımı aşağıda Şekil 13.1'de gösterilen grafikte verilmiştir.



Şekil 13.1. Endüstriyel Kontrol Sistemlerinde Zafiyeti Bulunan Ürünler [2]

Siber Güvenlik açısından kritik altyapıların başında gelen enerji sistemlerini siber tehditlerden korumak üzere tüm dünyada yoğun çalışmalar ve önemli ölçüde yatırımlar yapılmaktadır. Uluslararası standart kuruluşlarınca çeşitli standartlar oluşturulmuş olup ISO/IEC 27001 (Information Security Management), IEEE 1402 (Electric Power Substation Physical and Electronic Security), IEC 62351 (Data and Communication Security), NERC 1300 (Cyber Security Standards), NERC CIP ve NISTIR 7628 (Smart Grid Cyber Security) bunların en önemlilerinin başında gelmektedir. Ülkemizde bu standartların bazıları Türkçe diline çevrilmesine rağmen bu standartlara uygun olarak siber güvenlik önlemlerini ve altyapısını uygulamaya geçiren elektrik dağıtım şirketi henüz yoktur. Daha da kötüsü, teknolojik sistem tedarik şartnamelerinde, siber güvenlik çözümünün yine yurt dışı tedarikçiler tarafından karşılanacağı varsayılmakta, dolayısı ile ulusal kritik altyapılarımız gelişmiş siber saldırılara karşı yine korunmasız duruma düşmektedir.

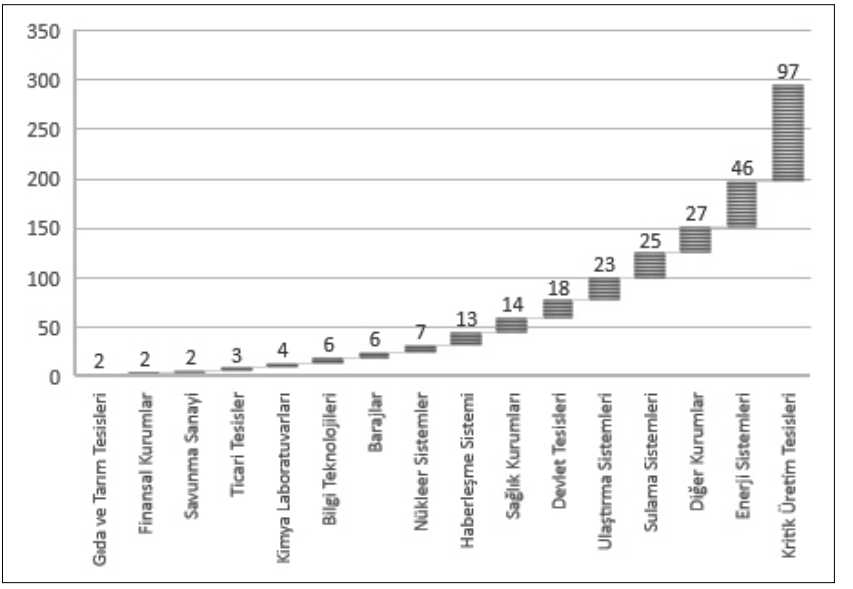
Günümüzde yaygınlaşan elektronik ve haberleşme teknolojilerinin kullanımıyla birlikte siber saldırı olayları da artmaktadır. Bununla beraber, olumsuz bir durumda zafiyetlerin ve sonuçlarının günlük hayatın akışını durduracak kadar etkiye sahip olan enerji sektörü bir ülke için büyük öneme sahiptir. Bu yüzden, çalışmada elektrik

enerjinin üretim, iletim ve dağıtımını ilgilendiren siber saldırı ve güvenliğine değinilecektir.

Güç sistemlerine karşı oluşabilecek siber saldırıların olasılığı, saldırıların sıklığı ve şiddeti gelişen şebeke altyapısı ile orantılı olarak artmaktadır. 2015 Küresel Bilgi Güvenliği Araştırması, dünyanın dört bir yanındaki enerji şirketlerinin, bir önceki yıla göre tespit edilen siber olayların sayısında altı kat artış olduğunu bildirmektedir. Endüstriyel Kontrol Sistemleri Siber Acil Müdahale Ekibi (EKS-SAME) tarafından rapor edilen enerji sektöründeki olayların sayısı oldukça önemlidir. Güç sistemlerinde, 2014 yılında 79 (en fazla rapor edilen siber saldırı olayı), 2015 yılında 46 olay (sektör başına en çok bildirilen ikinci olay), 2014 mali yılında tüm sektörlerde rapor edilen 245 toplam olayın %55'i "Gelişmiş ısrarlı tehditler (GIT) veya karmaşık aktörlerden oluşmuştur. Olayların yaklaşık %38 "bilinmeyen" bir erişim vektörü olarak sınıflandırılmıştır. Bu durumlarda, güç sisteminin tehlikeye girdiği onaylanmıştır, bununla birlikte, adli kanıtlar, haberleşme ağda ele geçirilen algılama ve izleme yeteneklerinin eksikliği nedeniyle izinsiz giriş için kullanılan başka yöntemleri işaret etmiştir. Bu durum, tespit edilen tehdidin ortadan kaldırıldığına işaret etmediği, böylece siber saldırıların çok karmaşık bir özelliğe sahip olduğunu göstermektedir. Şekil 13.2'de gösterilen grafikte olduğu gibi, bir önceki yıla benzer olarak 2015 Yılı'nda da tüm sektörler arasında rapor edilen 295 olaydan, erişim vektörlerinin yaklaşık %37'si bilinmeyen olarak belirtilmiştir. 2017 yılı içerisinde; 1.550 Kuruma siber güvenlik bildiriminde bulunulmuştur. 1.567 kritik ve acil olarak ele alınması gereken zafiyet bildirimi yapılarak internete açık servislerde 1.500'ün üzerinde açıklık tespit edildi ve alınması gereken tedbirlerle birlikte ilgililerine iletildi, ayrıca 2017 yılında siber saldırıların, bir önceki yıla göre 11 kat artmıştır.

EKS-SAME, enerji sistemleri sektörü katılımcılarına elektrik, petrol ve doğalgaz tesisleri dahil olarak kurulan ortaklıkların, diğer kritik üretim tesislerine kıyasla, aldığı olay raporlarının sayısına katkıda bulunduğunu belirtmektedir. 2017 tarihli Küresel Bilgi Güvenliği Araştırması, enerji ve güç sistemleri şirketlerinin yüzde 80'inin mobil bilgisayarlar, kötü amaçlı yazılım ve kimlik avının en büyük endişe kaynağı, siber tehditlerde yaşanan artış olduğunu belirtti. Siber saldırıların giderek daha karmaşık hale gelmesi nedeniyle, mevcut

siber tehditleri ele alarak gerekli tedbirleri almak yeterli derecede korumayı sağlamamakta, aynı zamanda güç sistemi gelecekte oluşabilecek yeni bir saldırıya karşı savunmasız kalabilir. Bundan dolayı, güç sisteminin temel bileşenlerinin bir bütün olarak tanımlanması ve korunması gerekmektedir.



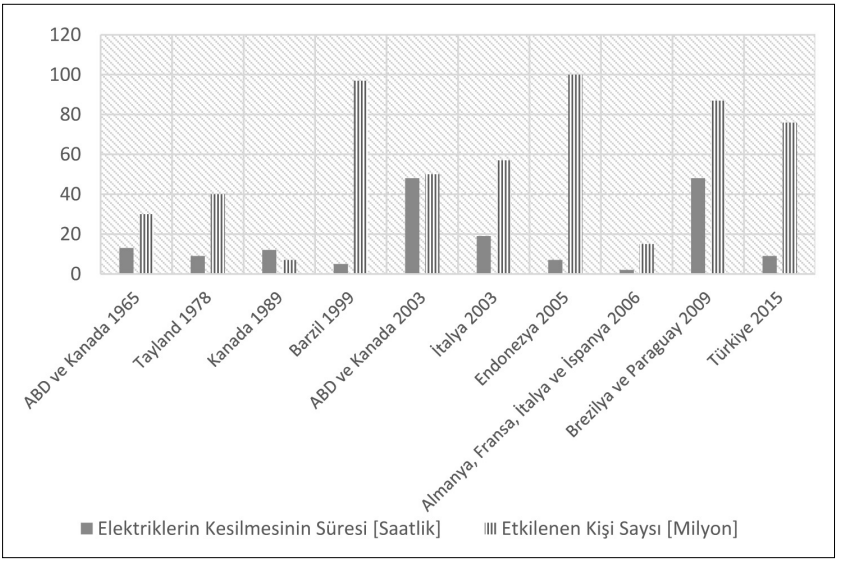
Şekil 13.2. Sektör bazlı yaşanan olayların dağılımı.

13.3. Güç Sistemlerinde Sürdürülebilir Enerji ve Arz Güvenirliği

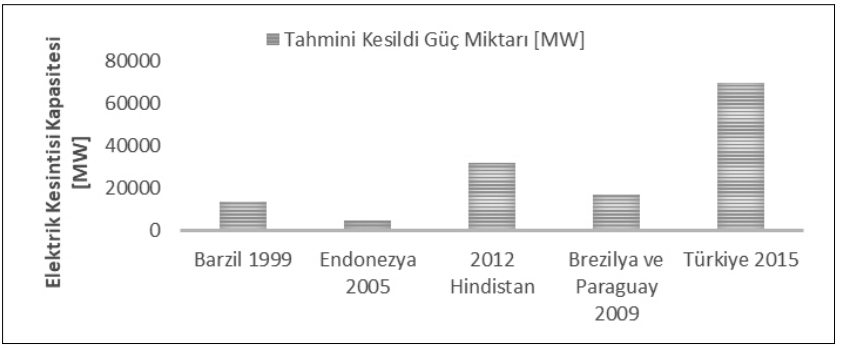
Enerji sürdürülebilirliği elektrik şebekesinin altyapısına oldukça bağımlıdır. Ulusal güç sistemindeki mevcut şebeke yapısında haberleşme, bilgi ağı üzerinden sağlanmaktadır. Yapılan bu haberleşme sistemine bağımlılık, kaçınılmaz olarak şebekeyi, siber saldırılar gibi iletişim ve ağ sistemleri ile ilgili olası zayıf noktalara karşı savunmasız bırakmaktadır.

Avrupa'da yaşanan büyük ölçekli enerji kesintilerinin ardından, ülkeler enerji kalitesini artırmak, enerjide arz güvenliğini sağlamak, karşılıklı haberleşme sağlanarak sürdürülebilir enerjiyi tüketiciye sağlamak ve siber saldırılara karşı şebekeyi korumak amacıyla akıllı şebeke sistemlerine yönelmişlerdir.

Dünya çapında yaşanan önemli kesintilerden dolayı doğrudan veya dolaylı olarak etkilenen tüketicilerin sayısı ve yaşanan kesintilerin süresi Şekil 13.3 (a)'da görülmektedir. Geçmişte yaşanan bazı büyük elektrik kesintilerindeki kaybedilen güç kapasiteleri dağılımı Şekil 13.3 (b)'de gösterilmiştir.



(a): Geçmişte yaşanan önemli kesintilerden etkilenen tüketicilerin sayısı ve süreleri



(b): Geçmişte yaşanan büyük elektrik kesintilerinin güç değerleri

Şekil 13.3. Elektrik kesintileri

Günden güne artan Yenilenebilir Enerji Kaynakları (YEK) kullanımı, bir taraftan doğaya salınan CO2 emisyonlarını azaltırken, diğer taraftan arz güvenliğini artırmaktadır. YEK'ler güç sistemine sağla-

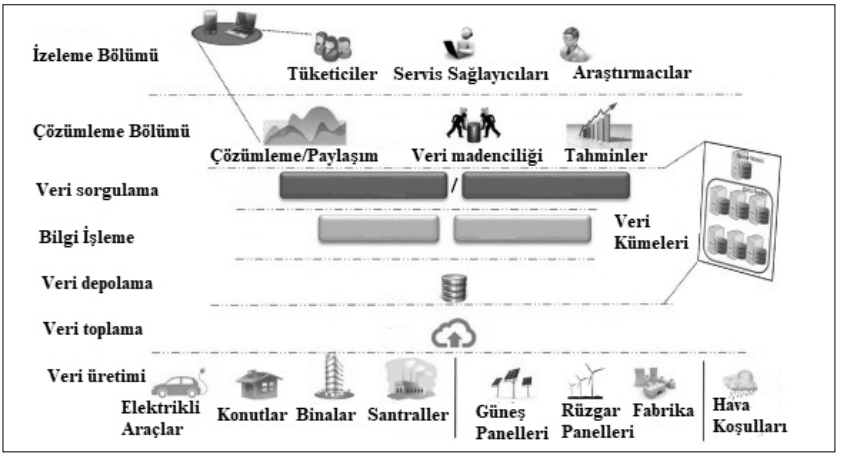
dıkları bu olumlu katkılara karşılık, iletim ve dağıtım şebekelerinde ilave bazı belirsizliklere ve tahmin edilemeyen olaylara neden olmaktadır. Tüketiciler için sağlanan büyük miktardaki elektrik enerjisinin ekonomik bir fiyat ile depolamasının imkânsızlığı, sistem operatörlerini üretim arzını gerçek zamanlı müşterilerin talepleri ile dengelemek gibi zorlu bir göreve yoğunlaştırmaktadır. Dağıtık Üretim (DÜ) içeren güç sistemlerinde; iletim, dağıtım ve dönüşüm ile ilgili kayıplarda azalma yaşanmasına rağmen, sistemin verimli bir biçimde işletilmesi, kontrol edilmesi ve siber saldırılara karşı korumak için oldukça karmaşık çözümler gerekmektedir.

Son yıllarda elektrik talebinde gerçekleşen hızlı artış hem enerji üreticileri hem de sistem operatörleri açısından bazı zorlukların ortaya çıkmasına neden olmuştur. Ayrıca gelecekte sadece ulaştırma sektörünün elektrifikasyonu ve bina ısıtma sistemlerindeki artışa bağlı olarak bu sorunların daha da artması beklenmektedir. Artan yüksek enerji talebini karşılama gereksinimi, geleneksel enerji santrallerine ek yük oluşturmaktadır. Pratik olarak, güç sistemi altyapısı, elektrik sisteminde ortaya çıkan yeni senaryoların neden olduğu ihtiyaçları ve artan karmaşıklığı tam olarak karşılayamamaktadır. Bu nedenle, otomatik ve dağıtılmış bir enerji dağıtım şebekesi oluşturmak için iki yönlü enerji ve bilgi akışı sağlamak günümüzün modern elektrik sistemleri için büyük bir gerekliliktir. Bu konseptte gerçek zamanlı veri toplanması ve işlenmesi için Bilişim ve İletişim Teknolojileri (BİT) temel unsurdur. İlgili tüm bu konular akıllı şebeke konseptinin temelini oluşturmakla beraber Siber Saldırılara karşı ciddi gereksinimlerin olduğunu göstermektedir.

Akıllı şebekeler, daha güvenli, sürdürülebilir ve uygun maliyetli ve aynı zamanda yüksek arz güvenliği ve kalitesine sahip elektrik tedarikini sağlamak üzere Şekil 13.4'te gösterildiği gibi yeni aktörlerin ve senaryoların bir araya getirildiği geleneksel elektrik şebekelerinin gelişimini temsil etmektedir.

Akıllı bir şebeke, elektrik şebekesinde Bilgi ve İletişim Teknolojileri yoluyla elektrik üretimini, dağıtımını ve tüketimini optimize eden akıllı bir elektrik şebekesi olduğu Şekil 13.4'ten anlaşılmaktadır. Özünde, akıllı şebekeler onları yönlendiren bilgi sistemlerinde büyük değişiklikler getirmektedirler. Elektrik şebekesinden gelen yeni bilgi akışları, merkezi olmayan yenilenebilir enerjiler üreticileri gibi yeni oyuncular, elektrikli araçlar ve bağlantılı evler gibi yeni kulla-

nımlar ve yeni iletişim araçları, akıllı sayaçlar, sensörler ve uzaktan kumanda noktaları bu sistemin birer bileşenidir. Bütün bu teknolojik gelişmeler, enerji şirketlerinin yüzleşmek zorunda kalacağı bir veri sızıntısına ve siber saldırıların gerçekleşmesine neden olacaktır. Büyük veri teknolojileri, kamu hizmetleri için uygun çözümler sunar, ancak büyük veri teknolojisinin kullanan güç sisteminin korunması oldukça önemli bir konu haline gelmektedir.



Şekil 13.4. Akıllı şebekelerdeki enerji ve büyük veri akışı

Dünyada pek çok ülke mevcut elektrik şebekesi modelini değiştirmek ve geliştirmek için birtakım önlemler almaktadır. Akıllı şebeke modelini önemseyen ülkelerin başında gelen ABD'nin akıllı şebeke yatırımlarının tutarı 2015'te yaklaşık 197 milyar doları bulmuştur. Batı Avrupa, 2027'ye kadar akıllı şebeke altyapısına 133,7 milyar dolar yatırım yapmayı planlamaktadır. Washington merkezli bir firma, Almanya'nın akıllı şebeke altyapısına yaptığı yatırımın 2016-2026 yılları arasında 23,6 milyar dolara ulaşacağını öngörmektedir. Bu ülkelerin yanı sıra Hindistan, Çin, Kore, Brezilya, Avustralya ve diğer dünya ülkelerinin, akıllı şebekeye yatırım yapan ülkeler gibi çeşitli projelerle mevcut şebekelerini teknolojik gereksinimlere göre geliştirme çabasında oldukları görülmektedir.

13.4. Enerji Sektörü, Güç Sistemleri Bileşenleri ve Siber Güvenlik Riskleri

Enerji Sektörü, elektriği verimli bir şekilde üretmek, taşımak ve dağıtmak için, "hesaplamalı algoritmaların ve fiziksel bileşenlerin

kusursuz entegrasyonuna dayanan mühendislik sistemlerine" sahip olan modern sistemlere bağımlıdır. Güç sistemlerinin modern siber-fiziksel sistemleri, ekipmanın fiziksel işlemlerinin dijital kontrolünü sağlayan EKS içerir. Rüzgâr Türbinleri gibi üretim santralleri sadece mekanik olarak çalıştırıldığı yerlerde, ekipman artık EKS tarafından çoğunlukla otomasyon sistemi ile bazen de uzaktan kontrol edilir. Bu teknolojik gelişmeler, gelişen şebeke altyapısının gelen siber saldırılara karşı giderek daha savunmasız kalmasına neden olur. Yeni dijital otomasyon veya akıllı şebeke teknolojilerini birleştirmek için eski şebeke sistemi bileşenlerinin modernizasyon çabaları, şebeke ağlarına daha fazla sayıda İnternet protokolü (IP) etkin erişim noktası getirmiştir. BİT ve işletim teknolojisinin (İT) EKS'ye entegrasyonu, sistemlerin daha büyük bağlantılarının bir sonucu olarak birçok tehdit vektörünü tanıtarak siber tehdit olasılıklarını genişletmektedir. İnternet ağları gün geçtikçe daha az güvenli hale gelmektedir. Uzaktan erişilebilen güç sistemi bileşenleri, korunmasız ağlar veya Internet üzerinden kamuya açık bir şekilde daha savunmasızdır. Elektrik şebekesinin her bir sistemi (üretim iletimi ve dağıtımı), aşağıdaki bölümlerde açıklandığı gibi fiziksel siber varlıklar aracılığıyla elektriğin güvenilir şekilde iletilmesi için benzer ve farklı güvenlik açıkları oluşturmaktadır.

Kritik süreçleri ve fiziksel fonksiyonları izleyen ve kontrol eden BİT ve ağ tabanlı sistemler, hassas altyapının diğer sektörlerinde olduğu gibi, elektrik sektöründeki temel işlemleri gerçekleştirmede büyük bir öneme sahiptir. Güç sistemlerindeki işlemler birden fazla EKS sisteminden oluşur (her bir güç sistemi sektörü, üretim- iletim-dağıtımını ve kontrolünden oluşmaktadır) ve bu sistemlerin her birinin işlevi birbirinden bağımsız olmasına rağmen benzer güvenlik açıklarına karşı duyarlı olabilir. Temel olarak bu güvenlik açıkları aşağıda belirtilmektedir:

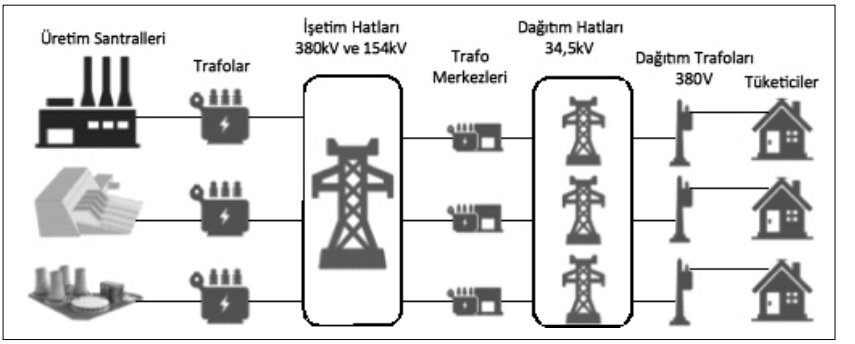
- Tehdit aktörleri atak yapmak için zaman uzaktan kullanılabilecek çeşitli giriş noktaları ve yolları,
- Sistem bileşenleri veya entegrasyon yoluyla gelişen EKS ile artan sayıda yeni güvenlik açıkları,
- İnternet'e doğrudan bağlı cihazlar dahil olmak üzere, daha fazla noktaya bağlı olan bileşenler üzerinden sistemlere ve ağlara daha kolay erişim sorunu,

- Kamu kurumları, piyasa koordinatörleri ve müşteriler arasında hassas veri toplama ve değişim (ekipman işletme durumu, güç üretimi ve tüketimi, elektrik fiyatlandırması, vb.) için daha fazla ek ağ yolları ve bağlantı gereksiniminin oluşturduğu açıklar.

Yaygın saldırı atakları karşısında, riskleri hafifletmek için çalışan birçok yardımcı program bilinmektedir, fakat güvenlik açıkları statik olmadığından dolayı siber varlıklar sürekli olarak izlenmeli ve değerlendirilmelidir. Tehdit eden bir aktörün becerisine veya yeteneklerine bakılmaksızın, bir yardımcı programın İT ortamına nasıl erişilebileceğini ve en iyi sonuçların hangi yol ile elde edilebileceğini anlamak, uygun etki azaltmalarını geliştirmek için gereklidir.

13.5. Güç Sistemlerinde Şebeke Bileşenleri ve Siber Saldırılar

Elektrik güç sistemlerinde, akıllı elektronik cihazlara (AEC) yönelik işlemleri yürütmek için çift yönlü iletişim modeli kullanmak gerekmektedir. İlerleyen teknoloji ile paralel olarak giderek artan bir şekilde EKS destekli bir endüstri sistemlerin kullanımı zorunlu haline gelmektedir. Böylece yeni siber güvenlik endişeleri ortaya çıkmaktadır. Siber hijyen, görünüşte en az zor olan savunmasızlık ve artan bağlantı noktaları gibi konuları içermektedir ve tehdit eden aktörler için çekici bir saldırı modunu oluşturmaktadır. Bu, saldırganlara eski teknolojideki klasik şebeke modelindeki güvenlik açıklarını sürekli olarak hedefleme veya yeni bağlantı modellerinde kötüye kullanım sağlama ya da gerektiğinde koordine edilmiş siber-fiziksel saldırı izleme fırsatı sunar. Klasik şebeke modelleri, siber-fiziksel teçhizatı etkilemeye yönelik kötü niyetli saldırıların ideal bir hedefidir. Çünkü üretim, iletim ve dağıtım tesisleri sürekli iletişim halinde olmaları, muhtemel en büyük ve en zararlı vakaları yaşaması için uygun bir zemin oluşturmaktadır. Bu durum, üretim, iletim ve dağıtım sisteminin saldırıya karşı dayanıklılık kazandığı anlamına gelmez. Elektrik şebekesine yönelik siber-fiziksel tehditleri anlamak için, şebeke sistemlerinin tek tek ve birlikte nasıl çalıştığını ve her sistemin genel olarak şebekeye ne tür güvenlik açıkları oluşturduğunu anlamak önemlidir. Aşağıdaki Şekil 13.5'te, güç şebekesi sistemlerini ve üretim, iletim ve dağıtım arasındaki bölünmeyi kısaca göstermektedir.



Şekil 13.5. Güç sistemi bileşenleri ve birimler arası bağlantı modeli

Genel olarak elektrik şebeke modelleri üç ana bileşenden oluşmaktadır: Klasik şebeke modelinde, sistemini oluşturan üretim, iletim ve dağıtım kısımları bulunmaktadır. Ayrıca, trafo merkezi gibi özel tesisleri ile beraber çalışan ve bazıları dağıtım sistemi seviyesinde olan birden fazla gerilim seviyesi içeren hatlar bulunabilir.

Elektrik güç sistemleri, kontrol sistemleri tarafından sağlanan otomasyon, uzaktan kumanda ve veri toplama yeteneklerinin bir sonucu olarak birçok işleve sahiptir. Fakat bu işlemlerin iletişimini sağlayan bağlantılarda hassas operasyonlar ve ağ varlıkları siber sızma ve manipülasyona da maruz bırakmaktadır. Modern dijital teknolojinin, dijital olarak bağlanacak şekilde tasarlanmamış eski ekipmanlara eklenmesi veya analog ekipmanın dijital olarak bağlanmış cihazlarla değiştirilmesi, önceden bağışık olan sistemlere karşı siber güvenlik açıkları oluşturmaktadır. Aynı zamanda, veri hırsızlığı veya finansal kayıpları kolaylaştırmaya yönelik BT sistemlerine karşı siber saldırıların tersine, İT sistemlerine karşı siber saldırılar, ayrıca görünüm, kontrol, güvenlik veya sensörlerin ve enstrümanların kaybolmasına ve manipülasyonuna neden olabilir. Elektrik piyasasında bu, ekipmanın arızalanmasına, fiziksel ekipman hasarına ve elektrik kesintilerine neden olması anlamına gelir. Ayrıca, her hizmet programı farklı bir sayıda ve çeşitli siber varlıklara sahiptir. Çok sayıdaki şebeke bileşeni, sistemler arasında siber güvenlik gereksinimlerinin tanımlanması ve uygulanması oldukça zordur.

Her bir şebeke katılımcısının siber güvenlik açısından konumunu belirleyen birçok değişken bulunmaktadır. Elektrik üretimi, iletimi ve dağıtımı dahilinde elektrik şebekesine yönelik siber tehditleri ayrı ayrı dikkate almak daha pratiktir. Her alanın güvenilir elektrik

üretim, iletim ve dağıtımı için farklı güvenlik açıkları vardır ve tüm alanlar benzer güvenlik açıklarını taşımaktadır. Siber saldırı riski taşıyan temel sistem işlevleri şunlardır:

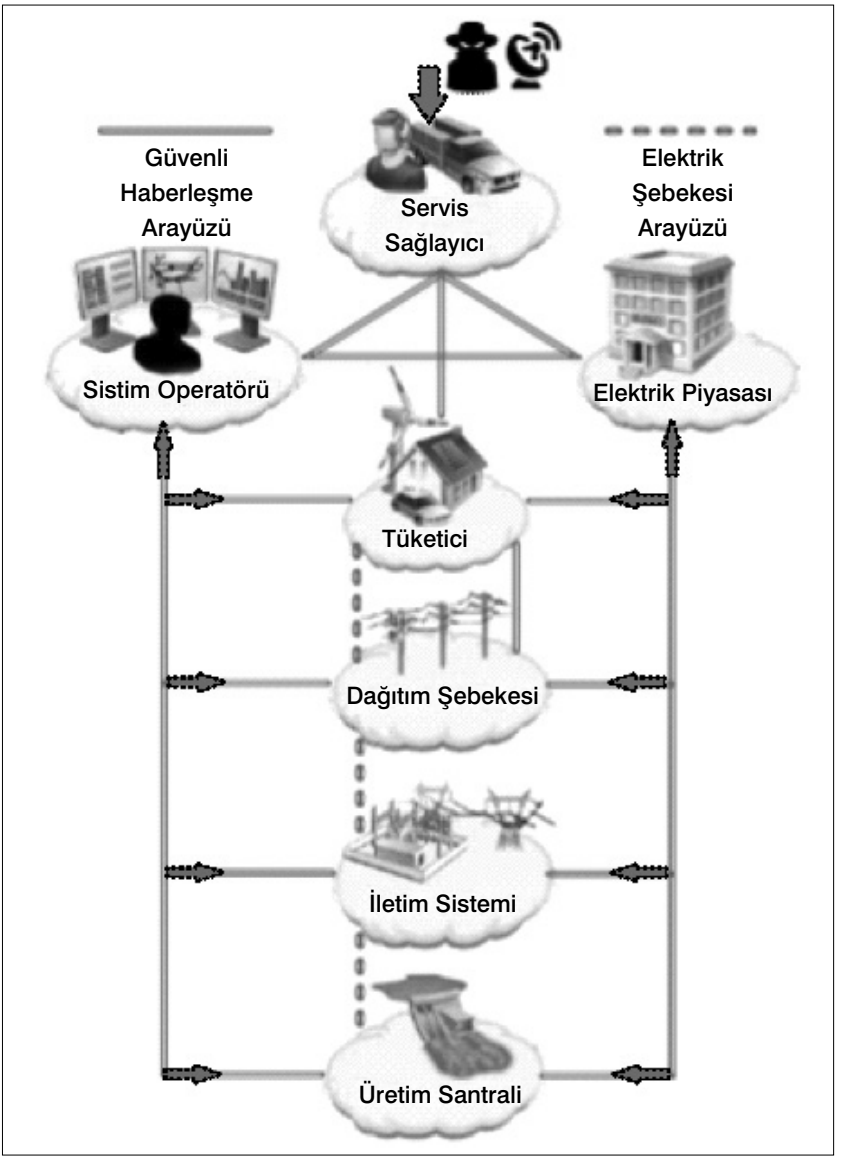
- Elektrik temini (üretim) veya transferi (iletim) stabilitesi,
- Ekipman performansı ve sistem onarma yeteneği (yedekleme sistemleri),
- Sistemler veya ekipman arasındaki iletişim,
- Üretim, iletim veya dağıtım ekipmanının çalışma koşulları ve
- Üretim ve dağıtım arasındaki güç aktarımdır.

Tablo 13.1. Alt sistemler ve bileşen başına saldırılar ve zarar maliyetleri

Alt Sistemler	Bileşen	Saldırı	Ölçü	Maliyet (K€)
İletim	Direkler	Fiziksel	Yıkma	50
	İletkenler	Fiziksel	Kısa devre	10
	İzolatörler	Fiziksel	Patlama	10
Trafolar	Yapı	Fiziksel	Yıkma	100
	Kontrol ve iletişim sistemi	Siber	İllegal Giriş	100
	Transformatörler	Fiziksel	Patlama	1000
	Kesiciler	Fiziksel	Patlama	100
Kontrol merkezi	Yapı	Fiziksel	Yıkma	1000
	Kontrol ve iletişim sistemi	Siber	İllegal Giriş	500
	Operatörler	Fiziksel	Kesme/İmha	1000

Siber saldırılar, bir sistem bileşenine saldırıyı hedeflediklerinde, bu saldırı altyapısı için bazı insan kaynaklarını ve sistem bilgilerini sağlamaları gerekmektedir. Birinci kaynağın bilgilerini elde etmek yüksek maliyetli fakat zor değildir, ikincisini ölçmek zor olsa da daha öngörülebilirdir. Her halükarda, bir sistem verisini sağlamanın hem parasal hem de parasal olmayan yönleri maliyet açısından ölçülmelidir. Saldırı için sistemin açıklarını gözetlemeleri ve kritik

noktaları belirlemeleri verecekleri tahribatın boyutunu artırmaktadır. Böylece, güç sistemindeki bileşenler, bulundukları yer, korum ve işlevsellik düzeyine göre kritik görevlere bağlıdır. Her bir bileşen başına atak yapmak için fiziksel kaynakların maliyetinin brüt ekonomik değerlendirmesi, Tablo 13.1'de verilmiştir.



Şekil 13.6. Siber saldırılara açık güç sistemi birimleri

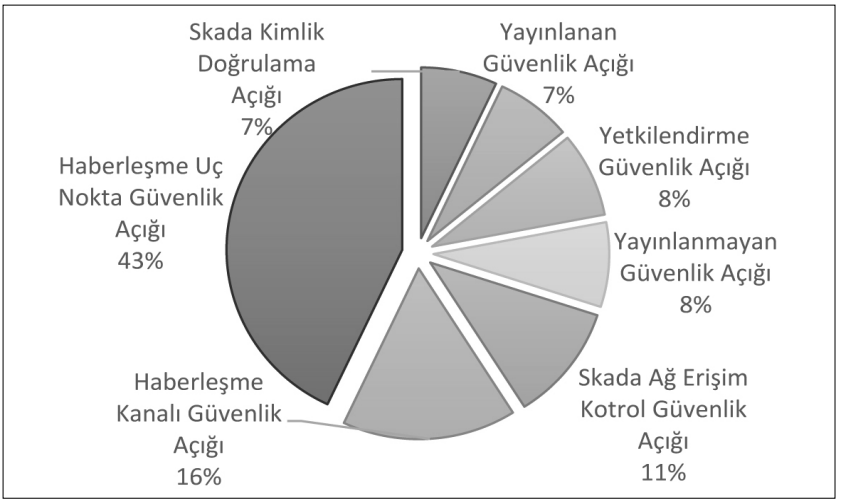
Şekil 13.6'da gösterilen güç sistemi modelinde gösterildiği gibi, sistem; güç üretimi, iletimi, dağıtımı, izleme, piyasa ve kontrol bileşenleri olarak karmaşık bir yapıdan oluşmaktadır. İletim hatları, baralar ve transformatörler gibi güç dağıtım elemanları, üretim noktalarından yüklere güç sağlar. Ancak, koruma tertibatları ve devre kesiciler gibi izleme ve kontrol cihazları, anormal koşullar altında hatalı elemanları şebekeden ayırmaktan sorumludur. Teknolojideki ilerlemeden dolayı, güç ağları kontrol ve SCADA sistemleri kullanılarak uzaktan kontrol edilebilir. Uzaktan kontrol ve denetim sistemi siber saldırganlar karşı savunmasız bırakabilir. Bu sistemlerin korumasız olması şebekeyi tehlikeye atabilir ve bileşenleri güç şebekesinden izole edebilir. Böyle bir durumda ciddi yük kayıplarına neden olan basamaklı kesintilere neden olarak büyük kayıpların yaşanması sonucu ortaya çıkacaktır. Şekil 13.6'da siber saldırılar ile karşı karşıya kalabilecek bileşenler ok işareti ile gösterilmektedir.

13.5.1. Güç Sistemlerinde Üretim Bileşenine Yönelik Siber Saldırılar

Elektrik, yeryüzünde ihtiyaç duyulan en önemli enerjidir ve ülkelerin büyümelerini tam anlamıyla etkileyen stratejik bir özelliğe sahiptir. Elektrik enerjisini kesintisiz bir şekilde tüketiciye ileten ve dağıtan şebekelerde meydana gelebilecek sorunlar, toplumun refah seviyesini ve gelişen sanayi ekonomisini doğrudan etkilemektedir. Gelişmiş veya gelişmekte olan ülkelerde, enerji üretim santralleri, iletim ve dağıtım şebekeleri ve diğer sistemler, önemli olan bütün altyapıları doğrudan etkileyen en kritik unsurlardır. Tüm bu unsurlardan dolayı enerji piyasasının tabii yapısından dolayı sahip olduğu olumsuzluklar, sistem yöneticilerin mutlak surette dikkate alması gereken çözümleyici işlemlerin başında bulunmalıdır.

Güç sistemleri, uzaktan kablolu ya da kablosuz olarak ağ yapısı verimi aktarımı yaptığından izleme ve kontrol işlemlerinde kullanılan verilerin güvenli bir şekilde yönetilmesi gerekmektedir. Dolayısıyla sistem güvenliğinin önemi artmaktadır. Idaho Ulusal Laboratuvarı'nın (INL) ABD Enerji Bakanlığı Elektrik Dağıtımı ve Enerji Güvenliği Dairesi'ne sunduğu raporda Ulusal SCADA Test Düzeneği (NSTB) programıyla ulusal enerji altyapısının siber saldırılar karşısında güvenliğinin ve esnekliğinin sağlanması hedeflenmiştir. Bu programın temel amacı SCADA sistemlerindeki gü-

venlik açıklarını analiz ederek saldırı etkisini hafifletme yaklaşımlarını tanımlayıp saldırılara karşı önlem almaktır. Raporda SCADA sistemine yönelik gerçekleştirilen siber saldırılarda istismar edilen güvenlik açıkları sınıflandırılmış ve analiz edilmiştir. İlgili raporun 2011 yılında yayımlanmış olmasına rağmen, içerdiği bilgiler ve elde edilen sonuçlar literatürdeki SCADA sistemlerinin siber güvenliği ile ilgili teknik çalışmalar içerisinde en kapsamlı olmasından ötürü bu tez çalışmasında ilgili yerlerde bu rapordan faydalanılmıştır. Şekil 13.7'de NSTB'e göre gözlemlenen güvenlik açıklarının çeşitlerine göre yüzdeleri verilmiştir. Dolayısıyla elektrik enerjisinin üretiminde, iletiminde ve dağıtımında tek bir güvenlik açığı diğer sistemlere oranla çok daha fazla kritik veya geniş kapsamlı olmaktadır.



Şekil 13.7. NSTB SCADA güvenlik açığı sıklığı

Elektrik enerjisini elde etmek için çeşitli enerji kaynakları kullanılır. Bunlar, Termik kaynaklar, Hidrolik Kaynaklar, Nükleer Kaynaklar, Güneş enerjisi, Rüzgâr enerjisi, Jeotermal Enerjisi, Gel-git (Med-Cezir) Enerjisi, Dalga enerjisi, Deniz sıcaklık gradyent enerjisi ve Hidrojen enerjisidir.

Elektrik temini, yukarıda sıralanan enerji kaynaklarının kullanımı sonucu ilgili santrallerden enerji üretimi ile başlar. Türbinlerle elektrik üretmek için yukarıda açıklanan yakıt kaynakları kullanılır. Yakıt kaynağından veya yöntemden bağımsız olarak, elektrik üretimi, çıkış ve frekansın geniş alan kontrolü (Otomatik Üretim Kontrolü -OÜK) ve yerel kontrolüne dayanır. Yerel kontrol döngü-

leri, jeneratör ekipmanına (türbinler gibi) komut gönderen odaları kontrol etmek için sürekli olarak veri besleyen sensörler içerir. Sonuç olarak, üretim talebi koşullarını karşılamak için üretim artırılır veya azaltılır ve sistem yükü kararlılığı, birden fazla üretim santrali ile dengelenir. Yerel kontrol döngüleri, büyük ölçekli coğrafi olarak dağılmış kontrol sistemlerine bağlı değildir. Bundan dolayı siber saldırı yüzeyinin, yerel kontrol sistemine erişim kazanmaya daha fazla odaklandığı düşünülmektedir. Bu durum, uzaktan erişim, kötü amaçlı yazılımın çeşitli yollarla tanıtılması veya kurumun kurumsal ağlarında güvenilir bir iletişim yolu aracılığıyla dönmesiyle sağlanabilir. Geniş alan kontrolü, haberleşmeye bağlıdır ve bu nedenle OÜK aşamasına yapılan bir saldırı, bir üretim tesisinden kaynaklanan güç stabilitesi üzerinde ciddi etkilere sahip olabilir, ancak OÜK işlevine ilişkin birden fazla saldırı vektörünün, güç akışını büyük ölçüde bozması gerekebilecektir.

Üretim kontrol döngüleri, ekipman güvenliği prosedürlerini başlatan (yani üretimde azalma, acil durumda kapatma), üretim ekipmanının arızalanması veya üretim ekipmanının fiziksel olarak imha edilmesini sağlayan istikrarsız güç yüküne odaklanmış saldırılara karşı savunmasız olabilir. Güç sistemlerindeki jeneratörün koruma röleleri, bağlı olan iletim sistemi ile senkronizasyon dışındayken üretim kaynağını bağlamak için manipüle edilebilir. İletim sisteminin daha büyük ataleti, sistemle senkronize edilmeye zorlandığı için dizel jeneratörü fiziksel rotoru üzerinde baskı oluşturur. Bu şekilde atak kısa bir süre boyunca hızlı bir şekilde gerçekleştirmek, bir siber kontrollü cihazdan üretim kaynağına fiziksel hasar verebilir.

Güç sistemi ekipmanına zarar veren başarılı bir siber saldırı olasılığı, bir rakibin fayda erişim kontrolleri, saldırı tespit yetenekleri, personel farkındalığı ve yedekleme önlemleri gibi bir dizi faktörü yenme yeteneğine bağlıdır. Güç şebekesinin büyük bir bölümünü etkilemek için, bir saldırganın eşzamanlı olarak çoklu üretim veya iletim olanaklarına erişim sağlaması ve bunlardan ödün vermesi, yardımcı kontrol merkezlerini hedeflemesi veya yaygın erişim sağlayan bir sisteme giriş yapması gerekecektir. Bununla birlikte, güç sistemlerinde, şu anda halen birbirine bağlı ve birçok alanda, kritik elektrik sistemi elemanlarında, sistem yeterliliğinde önemli ve yüksek maliyetli güncellemelere, siber güvenlik yatırımlarına, eşzamanlı siber olaylara karşı dirençli olmaları gerektirmektedir.

13.5.2. Güç Sistemlerinde İletim Bileşenine Yönelik Siber Saldırılar

Güç sistemlerinde enerjinin üretiminde dikkate alınan temel unsurlar, bu enerjinin olabildiğince düşük bir kayıp ile taşınması konusunda da göz önünde bulundurulur. Ayrıca, enerjinin güvenli olarak tüketiciler iletimi ve dağıtımı oldukça önemlidir. Bundan dolayı güç sistemlerindeki iletim ve dağıtım şebekesi kayıplarını en düşük seviyeye çekilmesi, enerjinin güvenilir ve verimli olarak yapılması tüm Dünya'daki gibi ulusal güç sistemimizde de gün geçtikçe önemi artmaktadır.

Elektrik üretildikten sonra, tüketiciye dağıtılmadan önce, çoğu zaman büyük coğrafi mesafeler boyunca voltajda kademeli olarak iletilir. İletim sistemlerinin ana bileşenleri, uzun mesafelerde elektriği daha verimli bir şekilde taşımak ve güç hatlarını bağlamak için aktarma kuleleri yüklemek için uygun gerilimler sağlamak amacıyla, adım-yukarı ve adım-aşağı gerilimi olan trafo trafolarıdır. Ayrıca, güç kaynaklarının üretim kaynaklarından dağıtılan sistem yüklerine ulaşmasını yöneten kontrol merkezleri bulunmaktadır. Bu unsurlar, iletim içindeki siber saldırılara karşı en riskli olanıdır, ancak transformatör fonksiyonlarını desteklemek için kullanılan yüksek voltajlı transformatörler ve diğer büyük ekipmanlar, değişim zamanı ve maliyet nedeniyle siber fiziksel bir olayda en etkili olanlardır.

Alternatif iletim yollarının olmaması veya birçok iletim aracında yedek transformatörlere erişim olmaması nedeniyle trafo kaybı riski artmaktadır. Bir transformatör hasarlıysa, üretilen güç, üretim kaynağına bağlı olan diğer alt istasyonlara veya bir yedek transformatör üzerinden yeniden dağıtılmalıdır. Bununla birlikte, çoğu jeneratörler sadece iki veya üç iletim tesisi tarafından sunulmaktadır. Bir jeneratörden güç yükünü alan bir trafo kaybı, kalan transformatörlere çok fazla stres koyabilir ve şebeke dengesizliği yaratabilir. Yedek transformatörler bu yükü hafifletebilir, ancak çoğu yardımcı program, siber bir olaydan zarar görmüş birini değiştirebilen yedek transformatörlere sahip değildir veya bunlara erişemez. Üretim kapasitesinin yetersiz olmasından kaynaklanan güç dalgalanmaları, şebeke boyunca ve uzun süreli elektrik kesintilerinde basamaklı arızalara neden olabilir. Ayrıca, bir transformatörün kaybı nadir olsa da yedeksiz bir kurtarma aylar sürebilir.

Modern alt istasyonlar, yerel fonksiyonları yönetmek için çeşitli iletişim türleri kullanmaktadır; güvenlik ihtiyaçları, trafo merkezlerindeki iletişimi kolaylaştıran Ethernet tabanlı ağlar olarak 1990'ların sonlarında yaygınlaşmıştır. Bir trafo merkezinin dijital işlemlerinin içine girildiğinde, gerekli beceri ve araçlara sahip bir saldırgan, iletişim ve kontroller için gerekli olan veri iletişimini bozabilir, bunlara uymaz ya da bunları etkileyebilir ve yük dengesizliğine neden olabilir. İzinsiz girişleri ve kötü amaçlı veri enjeksiyonu tanımlamak için algılama yetenekleri olmayan trafo merkezleri, bir saldırganın keşif olmadan zaman içinde birden çok alt istasyonunu işlemesine izin verebilir. Bu ağlarda, şebekenin bir bölümünü bozacak kadar güçlü koordineli siber saldırı riski daha yüksektir.

Üretime benzer şekilde, iletimden sorumlu kamu kurumlarına yönelik siber tehditler, bir trafo merkezi içindeki ağ yapılandırması ve veri iletişim araçları ve trafo merkezi ve iletim kulesi fiziki güvenliği gibi çeşitli değişkenlere bağlıdır. Şebeke boyunca güç aktarımını önemli ölçüde etkilemek için, bir saldırganın aynı anda birden fazla yüksek voltajlı iletim hattını veya transformatörünü kesmesi veya imha etmesi için karmaşık araçlar gerekir. Bu durum yüksek beceri ve kaynakların yanı sıra yerel ekipmana erişim ve devre dışı bırakma kabiliyetine de ihtiyaç duyacaktır, çünkü trafo merkezleri genellikle iletişim trafo merkezi kaybedilirse ve tüm ekipman normal şekilde çalışmaya devam edecek şekilde yapılandırılmıştır.

13.5.3. Güç Sistemlerinde Dağıtım Bileşenine Yönelik Siber Saldırılar

Elektrik dağıtımı ve yerel teslimatı genellikle Güç sistemlerini bir parçası olarak kabul edilmez ve devlet kamu hizmeti komisyonları tarafından denetlenir. Bu durum, siber güvenlik standartlarının ve seçilen standartların uygulanmasının, dağıtım hizmetlerinin kapsamı ve koruma önlemlerinin genişliğine bağlı olarak değişebileceği anlamına gelir. Ancak bazı durumlarda, dağıtım unsurlarına yönelik siber saldırıların güç sistemlerine ulaşan sonuçları olabilir. Elektrik şebekesini etkileyecek şekilde dağıtım seviyesinde birçok teyit unsuru oluşabilmektedir. Olabilecek saldırı düzlemi olarak hizmet veren bir dağıtım sistemi üzerinden yapılabilmektedir. Dağıtım şebekesine yönelik atak yapak Siber saldırganlar, BT altyapısına erişmek için kötü amaçlı yazılım kullanabilirler, ardından SCADA da-

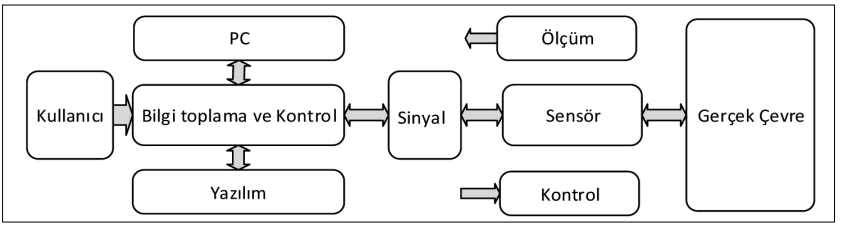
ğıtım yönetim sistemini içine sızarak, dağıtım elektrik altyapısında istenmeyen durum oluşturarak, enerji kesintilerine neden olduktan sonra SCADA sunucularını silerek geri yüklemeyi ertelemeye çalışabilirler. Siber Saldırganlar yüksek beceri seviyesini göstererek ve muhtemelen birkaç ay süren keşif ve birden fazla trafoyu eşzamanlı olarak birden fazla alt istasyona alan ve aynı anda 230 bin müşteriyi elektriksiz bırakan yedek santralleri devre dışı bırakan saldırıları yürütebilirler.

Bir dağıtım alt istasyonuna yapılan bir siber saldırı, kesintileri durdurmak için SCADA işlemlerini tehlikeye sokmak veya yük dengesizliğine neden olmak için kesicileri manipüle etmeyi içerebilir, ancak bu etkilerin yalnızca yerel hizmet alanı etkilerine sahip olacağından genel şebeke için çok az risk oluşturmaktadır. Ancak, Siber saldırılar bir dağıtım SCADA sistemine bir trafo merkezi üzerinden (fiziksel olarak) erişebiliyorsa, SCADA sistemi içindeki diğer dağıtım ve potansiyel olarak iletim elemanlarına erişime izin vermesi nedeniyle risk önemli ölçüde daha yüksektir. Ayrıca, iletim ve dağıtım sistemleri arasındaki adım düşürme transformatörleri gibi şebeke bağlantı noktaları her zaman siber güvenlik açıkları sunabilir.

13.6. SCADA Kontrol Sistemlerine Yönelik Siber Saldırılar

PC tabanlı basit bir Denetleyici Kontrol ve Veri Toplama (SCADA) kontrol sistemi Şekil 13.8'de görüldüğü gibi fiziksel sistem, algılayıcı ve kontrol elemanları, sinyal işleme, veri toplama ve kontrol donanımı ve bilgisayar yazılımı kısımlardan oluşmaktadır. SCADA sistemleri, kritik bir şekilde enerji üretim, iletim ve dağıtım sektörlerinin dokusuna derinden nüfuz etmiştir. Coğrafi olarak dağılmış sürekli dağıtım operasyonları üzerinden, bu bilgisayarlı gerçek zamanlı proses kontrol sistemleri, standartlaşmaları ve diğer ağlara bağlanabilirliklerinden dolayı, siber vasıtalar tarafından giderek daha fazla ciddi hasara ve bozulmaya maruz kalmaktadır. Bununla birlikte, SCADA sistemleri genellikle artan siber tehditlerden çok az korumaya sahiptir. Potansiyel tehlikeyi anlamak ve SCADA sistemlerini korumak için, standart BT sistemlerinden farklarını vurgulamak ve bir dizi güvenlik mülk hedefi sunmak gerekmektedir. Dahası, siber kaynaklı siber-fiziksel saldırı olduğunda SCADA sistemleri dahil olmak üzere olası siber saldırıların sistematik olarak

tanımlanmasına ve sınıflandırılmasına odaklanmak gerekmektedir. SCADA sistemlerinin kontrol performansı üzerindeki etkisinden yola çıkarak, saldırı kategorisi kriterleri, SCADA sistemlerini geleneksel Bilgi Teknolojisi (BT) sistemine karşı güvenceye almak için ortaya çıkan benzersiz zorlukları tanımlayan bu tür saldırıların ortak özelliklerini ve önemli özelliklerini vurgulanarak sistemin korunması sağlanmalıdır.



Şekil 13.8. Scada kontrol sistemi

Son olarak çalıştırma seviyesi kontrolleri operatör tarafından yapılır. Şekil 13.8'de santral otomasyon sistemi şematik olarak gösterilmektedir.

13.7. Siber Saldırılar ve Alınması Gereken Önlemler

Günümüzde kullanılan enerji şebekeleri giderek daha karmaşık bir hal almaktadır. Şebekede kullanılan modern cihazlar, operasyonel yöntemler ve iletişim ağlarından dolayı güç altyapısından istediğimiz güvenilirliği, esnekliği ve verimliliği korumak için yeni yöntemlere ihtiyaç duyulmaktadır. Güç sisteminin güvenilirliğinde yaşamsal önem taşıyan bir diğer husus, şebekenin siber güvenliğinin korunmasıdır. Güç sistemi koruma ve kontrol cihazlarına yönelik siber saldırılar temel olarak iki yönlü hasar oluşturmaktadır. Bunlar;

- Güç sisteminde kritik sonuçlar doğurabilecek enerji kesintileri,
- Şebekeye bağlı kullanılan ekipmanlara yönelik büyük ölçekli zararlar.

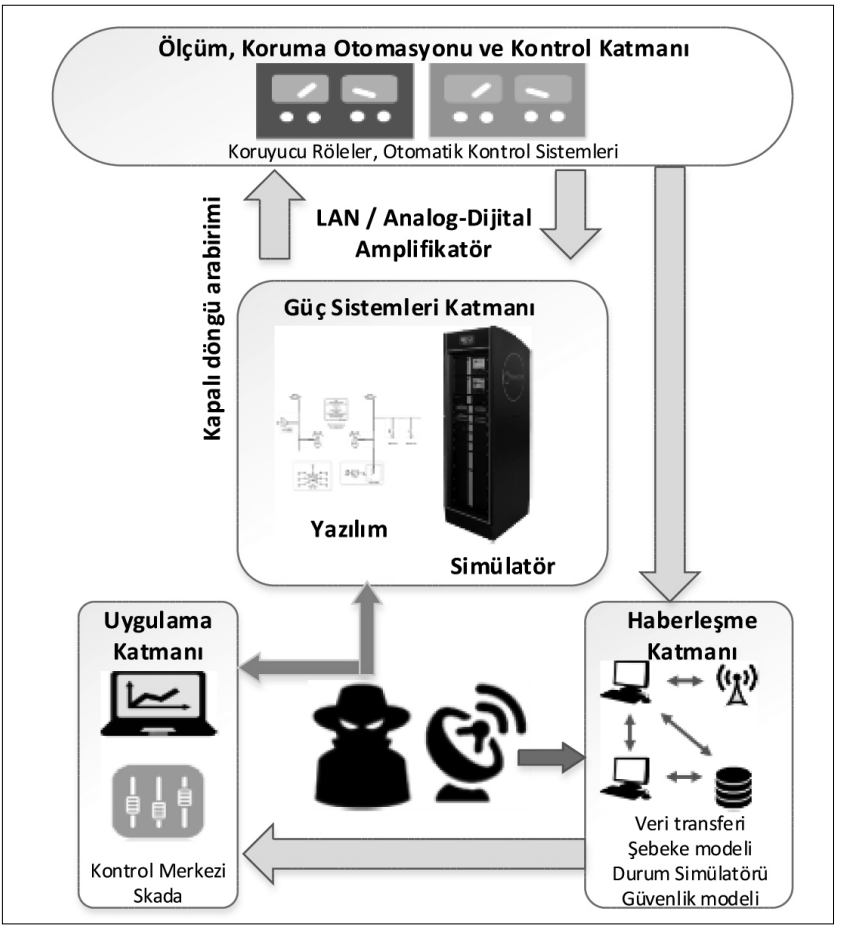
Uygun biçimde tasarlanmış ve uygulanmış siber güvenlik önlemleri, siber olayların önlenmesi ve güvenli bir hizmet için güç sisteminin kritik işlevlerini sürdürmeyi amaçlamaktadır. Akıllı şebeke laboratuvarlarında yapılacak simülasyonlarda, güç sistemleri için gerçek koruma, kontrol ve ölçüm cihazlarına bağlanarak uygula-

malar yapılabilmektedir. Bu uygulamalar, enerji sistemi güvenlik teknolojilerinin testlerinin gerçekleştirilmesi için gerçekçi, esnek ve kapsamlı bir test ortamı sağlayacaktır. Kurulması planlanan akıllı şebeke laboratuvarında benzer modelleme uygulamaları yapılarak, ulusal güç sistemimiz için siber saldırılara karşı koruma tedbirlerinin geliştirilmesine yönelik çalışmalara imkan sağlanacaktır. Aşağıda yer alan Şekil 13.9'da Akıllı şebeke laboratuvarında kurulması planlanan Siber Güvenlik Test Tabanlı Gerçek Zamanlı Simülasyonu gösterilmektedir. Önerilen akıllı şebeke laboratuvarında, aşağıdaki akıllı şebeke güvenlik sorunlarının incelenmesi planlanmıştır;

- **Kullanılabilirlik:** Bilgilerin zamanında ve güvenilir bir şekilde girilmesini ve kullanılmasını sağlamak, akıllı şebekede en önemli hususlardan birisidir. Bunun nedeni, kullanılabilirlik kaybı, güç dağıtımını zayıflatabilecek, bilgiye erişimin veya bilginin kullanılmasında aksaklık yaşanmasına sebebiyet verebilecektir. Bu aksaklılar proje kapsamında faaliyeti gerçekleştirilecek siber güvenlik modülü ile modellenebilecek ve ilgili sorun için çözümler üretilebilecektir.
- **Bütünlük:** Yanlış bilginin değiştirilmesi veya imhasına karşı korunmak, bilginin reddedilmesi ve özgünlüğün sağlanması ile gerçekleşecektir. Bütünlük kaybı, bilginin yetkisiz olarak değiştirilmesi veya yok edilmesi ve güç yönetimi ile ilgili yanlış karar verilmesine neden olabilmektedir.
- **Gizlilik:** Bilgi erişimine ilişkin yetkili kısıtlamaların korunması esas olarak kişisel gizlilik ve mülkiyet bilgilerini korumak için gereklidir. Bu durum, özellikle kişilere açık olmayan bilgilerin yetkisiz olarak ifşasını önlemek için gereklidir.

Kazanç sağlamak veya zarar vermek maksatlarıyla siber ortamda belirlenecek hedef ya da hedeflere yönelik gerçekleştirilecek faaliyetler siber saldırıları oluşturmaktadır. ABD Ulusal Araştırma Konseyi tarafından, 2009 yılında yapılan bir çalışmada siber saldırılar; "Haberleşme sistemleri, internet ağları ve bu ağda taşınan verilerin yapısını deforme etmek, dolandırmak veya ortadan kaldırmaya yönelik gerçekleştirilen planlı ataklar" olarak tanımlanmıştır. Saldırganlar siber saldırılarla, siber ortamdaki fiziksel veya sanal yapıyı, yazılım, donanım ve altyapı sistemlerini, genellikle de bu sistemler üzerindeki bilgiyi ve kullanıcıları hedef alarak eylemlerini gerçek-

leştirirken, temel olarak üç prensibe göre hareket etmektedirler. Bunlar, gizli bilgilerin elde edilmesi veya bilginin gizliliğinin açık edilmesi, bilgiye zarar verilerek değiştirilmesi yani bütünlüğünün bozulması ve bilgiye kullanıcıların erişiminin engellenmesi yani kullanılabilirliğinin önlenmesidir. Türkiye 2016-2019 Siber Güvenlik Stratejisi ve Eylem Planı belgesinde, bu üç prensipten hareketle siber saldırıların tanımı; "Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler" şeklinde yapılmıştır.



Şekil 13.9. Siber güvenlik test ortamında gerçek zamanlı benzetim

SCADA kontrol sisteminin güvenliğinin sağlanması kolay bir süreç olmayıp siber saldırıların artmasıyla birlikte kritik yapıların korunması büyük önem taşımaktadır. Siber riskleri azaltmak için fiziksel güvenlik önlemlerine nazaran ekstra güvenlik tedbirleri alınmalıdır. Endüstride bazı sistemler, güvenlik tedbirlerini uygulamak için gereken hizmet kesintilerinin bile yapılamayacağı kadar kritik olarak nitelendirilmektedir. Diğer yandan kontrol yazılımlarının bilgisayar temelli virüsler ortaya çıkmadan önce geliştirilmiş olması veya sistem sürümlerinin donanımsal şartlardan dolayı yükseltilememesi, anti virüs programlarının devre dışı kalmasına sebebiyet verdiğinden dolayı güvenlik sorunu ortaya çıkmaktadır. Ancak, kontrol sistemine ait yazılımın, güvenlik hususlarının yanında sistemi kullanacak operatörlerinde siber güvenliğinin sağlanması hususunda bilinçli olması ve aşağıda verilen adımları izlemesi gerekmektedir:

- Veri koruma yönergeleri, protokolleri ve politikalarının resmi hale getirilmesi ve tam olarak uygulanması,
- SCADA kontrolü ve ilgili firmaya ait hayati önem taşıyan bilgi ağlarının diğer tüm ağ bağlantılarından ayrılması,
- Kontrol ve SCADA sisteminin yer aldığı tüm ağ sistemine virüs ve güvenlik duvarı korumasının kurulması,
- Virüs ve güvenlik programlarının güncellemelerin periyodik olarak sürekli yapılması,
- İşletim sistemleri ve sunucuların güncellenmesi ve yapılandırılması,
- İzinsiz erişimlerin tespiti için güvenlik duçarı kayıtlarının denetlenmesi,
- Güvenlik testlerinin düzenli ve periyodik olarak gerçekleştirilmesi,
- Operatörlerin SCADA ve bilgi teknolojisi sistemleri ile ilgili veri koruma yönergeleri ve protokolleri konusunda eğitimli olmalı,
- Operatörlerin SCADA, bilgisayar ve kontrol sistemlerine erişim sağlarken özgün kullanıcı kimlikleri ve şifreler kullanmalı,
- Operatör ya da diğer yetkililerin görevinin sona ermesi ya da görevden ayrılması durumunda kullanıcı hesabının silinmesi,

- Kablosuz ağ erişimin sınırlandırılması ve yetkili kablosuz ağların mümkün olan en yüksek şifreleme düzeyinde korunması,
- Hesapta belirli bir süre işlem yapılmaması durumunda ağ otorumun sistem tarafından otomatik olarak kapatılması,
- Scada kontrol merkezine erişimlerin güvenli hale getirilmesi,
- SCADA sunucularının bulunduğu fiziksel mekanların güvenliğinin sağlanması,
- SCADA sistemin eksikliklerinin ya da aksaklıklarının periyodik olarak değerlendirilmesi,
- Sunucu, ağ bileşenleri ve hayati önem taşıyan çalışma istasyonları için kesintisiz güç kaynağının bulundurulması,
- Sistem yedeklerinin periyodik olarak alınması,
- SCADA ve diğer kontrol sistemleri ve ağlarının yalnızca yetkili kişiler tarafından erişime açık olması ve söz konusu personelin belirlenmesi,

- Başarısız oturum açma girişimlerine sayı kısıtlaması getirilmesi ve sayının aşılması halinde sistemin kilitlenmesi,
- Her girişte son başarılı giriş tarihi ve saatinin bildirilmesi,
- Tek kullanıcının farklı konumlarda oturum açmasının engellenmesi,
- Kontrol sistemi ile kablosuz bağlantılarının yönetilmesi ve denetlenmesi,
- Tüm güvenlik teknikleri ve teknolojilerinin yanı sıra tehditler, riskler ve son yaşanan olaylarla ilgili bilgi sahibi olmak için profesyonel topluluklar veya benzer şirketlerle iletişim halinde olunmalı,
- Operatörlere, belirli periyodik zamanlarda sürekli eğitimin verilmesi,

Alınacak teknik önemlerin yanında Güvenli Siber Alan oluşumu çerçevesinde karar alıcıların görev ve sorumlulukların belirlenmesinde ulusal bir plan geliştirilmeli, olay anında kriz yönetimi oluşturulmalı ve acil durum kurtarma planları oluşturarak yasal işlemlerin başlatılması için adli mercilerin bilgilendirilmesi gerekmektedir.

Enerji altyapısının işletilmesinden sorumlu olan kamu kuruluşları ve özel şirketlerin karşılaşabileceği siber tehditlere karşı önlem alabilmek için aşağıdaki hususların dikkate alınmasında fayda vardır:

- Tedarik edilecek kontrol sistemlerinin mümkünse kaynak kodunun tedarikçi firma tarafından verilmesinin sağlanması,
- Ülke genelinde birden fazla farklı teknoloji tedarikçisinin kullanılması sağlanarak tek bir siber saldırı yöntemi ile tüm ülke şebekesinin arz güvenliğinin tehlikeye düşürülmesinin engellenmesi,
- Teknoloji tedarikçisinin ürün güvenlik sertifikasyonlarının talep edilmesi,
- Bilişim Sistemleri ile Kontrol Sistemlerinin farklı güvenlik seviyesine sahip ağlar bazında birbirinden ayrıştırılması,
- Tedarik edilen sistemlerin siber güvenlik altyapısının yabancı tedarikçiler tarafından değil, akredite yerli güvenlik danışman şirketleri tarafından tasarlanması ve test edilmesi,
- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) ve diğer siteler tarafından yayınlanan zafiyet ve saldırıların takip edilerek gereken yama ve önlemlerin zamanında alınması,
- Dağıtım Şirketine ait bilişim ve otomasyon-kontrol sistemlerinin periyodik güvenlik testlerinin bu konuda uzman yerli şirketlere yaptırılması.

Enerji Sektörü için aşağıdaki düzenlemelerin ve uygulama esaslarının başlatılması da önerilmektedir.

- Milli SCADA Sistemlerinin geliştirilmesine yönelik AR-GE programlarının başlatılması,
- Endüstriyel Kontrol ve SCADA Sistemlerine yönelik Siber Güvenlik ürünlerinin milli olarak geliştirilmesi,
- Ulusal Akıllı Şebeke Siber Güvenlik Standartlarının oluşturulması ve kamu ve özel şirketlerin bu standartlara uygunluğunun denetlenmesi,
- Yabancı firmalardan tedarik edilen enerji otomasyonu ekipmanları ile SCADA yazılımlarının, ulusal bir merkezde güvenlik, gü-

venilirlik ve birlikte çalışabilirlik testlerinin yapılarak sertifikasyona tabi tutulması ve bu sertifikasyonu karşılamayan ürünlerin kullanımının yasaklanması,

- Her sene düzenlenen Siber Tatbikat Programına EÜAŞ, TEİAŞ ve EDAŞ'lara ait bilgi ve kontrol-kumanda sistemlerinin dahil edilmesi
- Ulusal Siber Güvenlik Kurulu çalışmalarında ETKB temsilcilerinin de katılması ve Endüstriyel Kontrol Sistemlerinin güvenliğinin ayrı bir başlık olarak ele alınması
- Siber Saldırılardan dolayı şebeke arz güvenliğinin tehlikeye düşmesi ve ilgili bölgedeki dağıtım şirketinin yeterli siber güvenlik önlemlerini almadığının tespiti durumunda Dağıtım Şirketlerinin bundan dolayı sorumluluk altına alınmasının sağlanması gerekmektedir.

Kaynaklar

[1] K., Tacettin. "Enerji Altyapılarının Korunması için Siber Güvenlik Stratejisi" Global Resources Partnership, 2 Nisan 2015.

[2] http://www.ptsecurity.com/download/SCADA_analytics_english.pdf

[3] Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015," PWC, September 30, 2014, accessed September 30, 2015.

[4] "NCCIC/ICS-CERT 2015 Year in Review," NCCIC and ICS-CERT, April 19, 2016, accessed July 21, 2016.

[5] "ICS-CERT Monitor September 2014—February 2015," ICS-CERT, March 11, 2015, accessed November 9, 2015.

[6] "NCCIC/ICS-CERT 2015 Year in Review," NCCIC and ICS-CERT, April 19, 2016, accessed July 21, 2016.

[7] "ICS-CERT Monitor September 2014—February 2015," ICS-CERT, March 11, 2015, accessed November 9, 2015.

[8] https://cleantechnica.com/2017/06/23/western-europe-smart-grid-investment-reach-133-7-billion-next-10-years-northeast-group-reports/

[9] Çaşın, M.H, "Kritik Enerji Altyapı Güvenliği Kavramı Kritik Altyapı Tesislerine Yönelik Potansiyel Tehditlerin Analizi Risk ve Tehdit Değerlendirmesi" Hazar Strateji Enstitüsü, Ocak 2015.

[10] Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, "NIST 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, May 2015, accessed May 1, 2016.

[11] "Challenges in Securing the Electricity Grid: Statement of Gregory C. Wilshusen," U.S. Government Accountability Office: Testimony before the Committee on Energy and Natural Resources, U.S. Senate Director Information Security Issues, July 17, 2012, accessed February 17, 2016.

[12] "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," U.S. Department of Energy and North American Electric Reliability Corporation, June 2010, accessed February 16, 2016.

[13] Assante, Michael J., and Robert M. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed February 24, 2016.

[14] Govindarasu, Manimaran, Adam Hahn, Peter Sauer, Cyber-Physical Systems Security for Smart Grid, Power Systems Engineering Research Center, February 2012, accessed February 25, 2016.

[15] "Interview with Manimaran Govindarasu" IEEE Smartgrid, July 2012, accessed February 24, 2016, www.smartgrid.ieeee.org.

[16] Dağ Funda, İşletim Sistemleri ve Bilgisayar Ağları, İstanbul, 2003.

[17] Parfomak, Paul W., "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations," Congressional Research Service, June 17, 2014, accessed May 4, 2016.

[18] Hurley Jr., Daniel C., James F.X. Payne, Mary T. Anderson, "Risk Mitigation in the Electric Power Sector: Serious Attention Needed," Armed Forces Communication and Electronics Association 2012, accessed February 25, 2016.

[19] Lee, Robert M., "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS ICS Security Blog, January 8, 2016, accessed March 2, 2016, www.ics.sans.org/blog.

[20] Sridhar, Siddharth, Adam Hahn, Manimaran Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," IEEE 100 (2012): 215, accessed February 25, 2016.

[21] Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat," Bipartisan Policy Center, February 2014, accessed March 3, 2016.

[22] Lee, Robert M., "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS ICS Security Blog, January 8, 2016, accessed March 2, 2016, www.ics.sans.org/blog.

[23] M. Unver, C. Canbay, "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik," 2010.

[24] R. Sanz, K. Årzén, "Trends in Software and Control," IEEE Control System Magazine, no. June, 2003.

[25] R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, "Security Strategies for SCADA Networks," Critical Infrastructure Protection, sayı 253, pp. 117–131.

[26] L. Yanfei, W. Cheng, Y. Chengbo, Q. Xiaojun, "Research on ZigBee Wireless Sensors Network Based on ModBus Protocol," Proceedings - 2009 International Forum on Information Technology and Applications, sayı 1, 487–490, 2009.

[27] Positive Technologies "SCADA Safety in Numbers" Report http://www.ptsecurity.com/download/SCADA_analytics_english.pdf

[28] R. Bayindir, Ş. Sağıroğlu, A. Özbilen, İ. Çolak, "Investigating Industrial Risks Based on Information Security for Observerable Electrical Energy Distribution System and Suggestions," Gazi University Journal of Faculty of Engineering and Architecture, 24: 4, 715–723, 2009.

[29] Q. Xiong et al., "A Vulnerability Detecting Method for Modbus-TCP Based on Smart Fuzzing Mechanism," IEEE International Conference on Electro Information Technology, 404–409, 2015.

[30] S. Bhatia, N. Kush, C. Djamaludin, J. Akande, and E. Foo, "Practical Modbus Flooding Attack and Detection", Conferences in Research and Practice in Information Technology Series, 57–65, 2014.

[31] W. L. Shang, L. Li, M. Wan, ve P. Zeng (2015). "Security Defense Model of Modbus TCP Communication Based on Zone / Border Rules: Misuse".

[32] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, ve D. Kundur (2015). "Implementing Attacks for Modbus/TCP Protocol in a Real-Time Cyber Physical System Testbed", Proceedings - CQR 2015: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability.

[33] G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T. Loix, ve H. Beitollahi (2009). "ICT Resilience of Power Control Systems: Experi-

mental Results from the Crutial Testbeds", Proceedings of the International Conference on Dependable Systems and Networks, 554–559.

[34] G. Dondossola, G. Deconinck, F. Garrone, ve H. Beitollahi (2009). "Testbeds for Assessing Critical Scenarios in Power Control Systems", 223–234.

[35] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, ve S. Hariri (2011). "A testbed for Analyzing Security of SCADA Control Systems (TASSCS)", IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT Europe, 1-7.

[36] B. Dutertre, "Formal Modeling and Analysis of The Modbus Protocol," Critical Infrastructure Protection, 189–204, 2007.

[37] A. Swales, "Open Modbus / Tcp Specification", Schneider Electric, 1–26, 1999.

[38] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack Taxonomies for The Modbus Protocols," nternational Journal of Critical Infrastructure Protection, 37-44, 2008.

[39] "MODBUS over Serial Line-Specification and Implementation Guide," 2002.

[40] T. H. Morris, "On Cyber Attacks and Signature Based Intrusion Detection for Modbus Based Industrial Control," 9: 1, 37–56, 2009.

[41] Glenn/Wright, "US Electric Utilities Cyber Security Threat Analysis," Idaho National Laboratory, March 2016, accessed March 20, 2016.

[42] "Energy Sector-Specific Plan 2015," Department of Homeland Security, accessed February 15, 2016.

[43] Hawk, Carol, and Akhlesh Kaushiva, "Cyber Security and the Smarter Grid," The Electricity Journal (2014): 89-90.

[44] "Booz Allen, Siemens and Power Analytics Partner with New York Communities to Win 16 NY Prize Microgrid Projects," Booz Allen Hamilton, McLean, VA, July 9, 2015.

[45] "Approaches To The Securıty Analysıs Of Power Systems: Defence Strategıes Agaınst Malicious Threats" E. Bompard Et. Al. European Commission Directorate-General Joint Research Centre Institute IPSC.

Siber Güvenlik Operasyon Merkezi

BÖLÜM 14

Mehmet TUNÇKANAT

SİBER GÜVENLİK OPERASYON MERKEZİ

Bu bölümde, sürekli ve gelişen BT tehditleri gözönünde bulundurularak Güvenlik Operasyon Merkezi (SOC) oluşturma ihtiyacı ve sağladığı katkılar ve sunulan hizmetin kapsamı gözden geçirilmiş, hizmet sunulan bu merkez açıklanmıştır.

14.1. Giriş

Kalıcı ve sürekli gelişen siber tehdit ortamı nedeniyle daha akıllı güvenlik çözümlerine ihtiyaç duyulmakta ve kurumlar da buna uygun harekete geçmektedir. Son küresel ekonomik yavaşlamaların ardından küçülen BT bütçelerine rağmen Gartner 2017 yılında güvenlikle ilgili test, yönetilen güvenlik hizmetleri, bilgi güvenliği alanlarını da içeren harcamaların 93 Milyar USD'dır [1].

Güvenlik operasyon merkezi (SOC) oluşturma güvenlik açıklarını azaltmak için etkili bir yoldur. SOC bilgi teknolojisi (BT) alanında tehdit izleme, tespit, olay yönetimi, müdahale, güvenlik raporlaması konularında çalışan insanları, süreçleri ve teknolojileri içermektedir. Bu kapsamda tamamen iç operasyon ve süreçler, teknolojiler ve kurum personeli bulunabileceği gibi dışarıdan görevlendirilmiş ve iç yetenekleri de içeren hibrit bir yapı da bulunabilir.

Özellikle yüksek miktarda veri işleyen, bu işlemler için karmaşık yasalara veya yönetmeliklere bağlı olan işletmeler, karmaşık siber saldırı risklerinden ötürü SOC oluşturmalı ya da yönetilen güvenlik hizmetini almalıdır.

SOC oluşturarak tehdit yönetimi faaliyetleriniz üzerinde ve kritik verilerinizin korunmasında daha fazla kontrol sağlayabilir ayrıca dış hizmetler alarak, örneğin küresel tehdit kalıpları gibi güvenlikle ilgili yetkinlilerinizi geliştirebilirsiniz.

Bu bölümde aşağıdaki konular detaylı olarak ele alınacaktır.

- Mevcut Güvenlik Operasyonlarınızın olgunluğu ve yeteneklerinin değerlendirilmesi
- SOC'larda ele alınması gereken beş temel işlev
- Her bir işlevin başarı ile gerçekleştirilmesi için atılması gereken adımlar

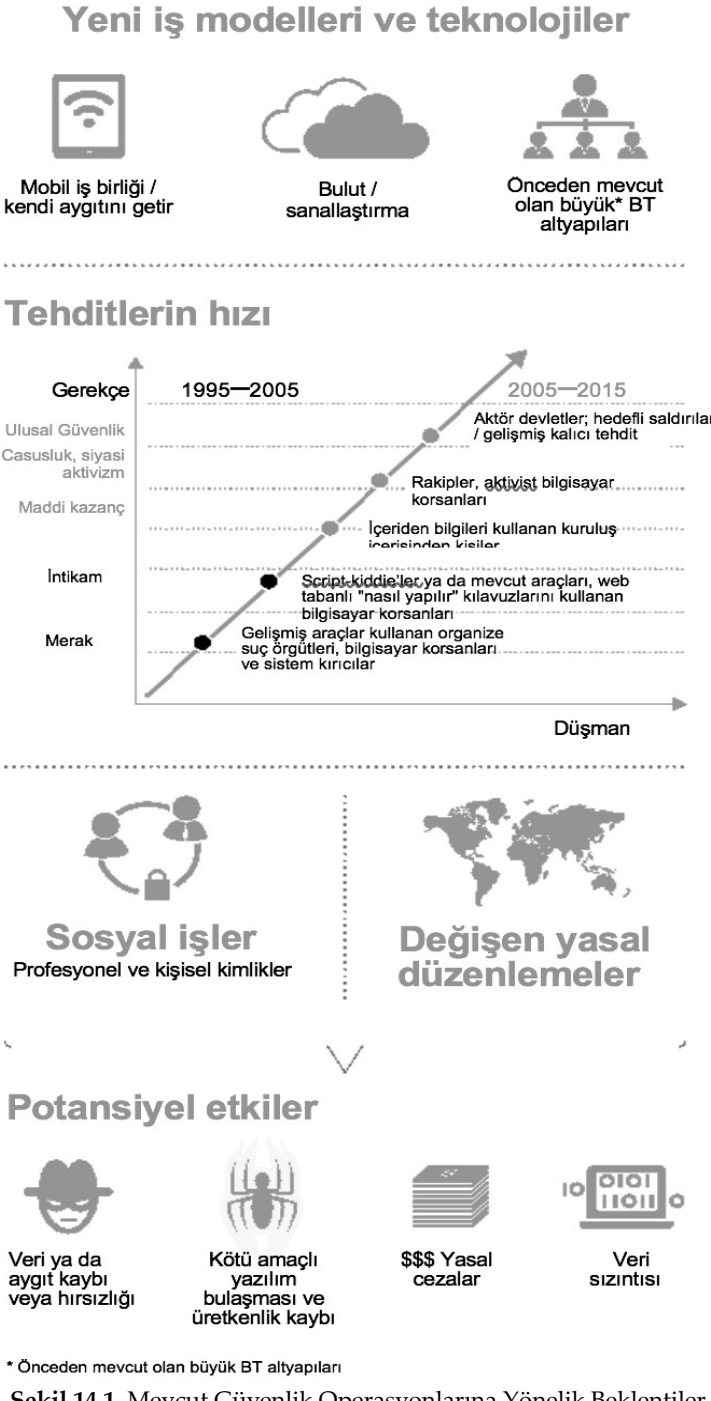
14.2. Güvenlik Sorunları

Tehdit ortamı, kuruluşun operasyonlarında hemen hemen her alanda risk teşkil ediyor. Aynı zamanda çeşitli yer paydaşlar arasında dağılan ve gün geçtikçe bulut tabanlı platformlar, mobil ağlar gibi yapılar üzerinde büyüyen karmaşıklık ve yapılandırılmış ve yapılandırılmamış verileri yönetmek gittikçe daha zor hale geliyor. En fazla saldırıya uğrayanlar en hassas kişisel müşteri verilerine sahip olanlar. Örneğin sağlık ve sosyal hizmetler sektörleri haftada 10.1 milyon saldırı, finans ve sigortacılık sektörü ise kabaca 3.6 milyon saldırı ile karşılaşmaktadır [2].

Şekil 14.1'de siber güvenlik operasyon merkezinden beklentiler kapsamı olarak verilmektedir.

Genel olarak baktığımızda "IBM Siber Güvenlik Endeksi" 2012 yılında 130 ülkeden 3.700 müşterisi üzerinde yaptığı detaylı güvenlik analizi çalışmalarında bilgiyi toplamaya, yok etmeye, değiştirmeye teşebbüs eden şüpheli 137.4 milyon olayı ortaya çıkarmıştır. Bu haftalık olarak 2.6 milyon ve günlük 380 bin saldırıya denk gelmektedir. Yapılan her 1 milyon saldırıdan %1.07'i si hedefine varmaktadır [2].

Ponemon Enstitüsü ABD'de güvenlik ihlali nedeniyle açığa çıkan her kayıt için 188USD ve toplamda bir kuruma ortalama yıllık maliyetin 5.4 milyon olarak tahminlemektedir [3]. Tabi bunun yanında müşteri verilerinin ele geçirilmesi şirketin imajının zedelenmesi, güvenirliliğin %21 düşmesi ortalama 332 milyon'a mal olmaktadır [4]. Kurumlar bu nedenle güvenlik tehditlerini yönetmekte daha kapsamlı yaklaşımlara ihtiyaç duymaktadırlar.



Şekil 14.1. Mevcut Güvenlik Operasyonlarına Yönelik Beklentiler

14.3. Güvenlik Operasyon Merkezi

Teknoloji, tehdit ortamındaki sürekli değişime gerektiği kadar hızlı uyum sağlayamamaktadır. Burada sorulması gereken soru, kuruluşunuzun saldırıya *uğrayıp uğramayacağı* değil, *ne zaman* saldırıya uğrayacağıdır. Ve bu saldırı gerçekleştiğinde, sahip olduğunuz kurumsal güvenlik operasyon merkezinin tehdidin etkisini azaltırken, niteliğini ve ciddiyetini hızla saptarken ve yönetime iş riskini etkin biçimde ele almaları için güvenlik istihbaratını sağlarken fark yaratıp yaratmayacağıdır.

Kurumsal güvenlik operasyon merkezi, tanımlı süreçler dahilinde çalışan ve tipik olarak bir ya da daha fazla şirket içi tesiste barındırılan bütünleşik güvenlik istihbaratı teknolojileriyle desteklenen uzman bir ekip olarak faaliyet gösterir. Genel güvenlik operasyonları ortamınız kapsamında faaliyet gösteren kurumsal güvenlik operasyon merkezi, özellikle siber tehditlere, izlemeye, adli soruşturmalara, güvenlik olayı yönetimine ve raporlamaya odaklanır.

Kurumsal güvenlik operasyon merkezleri aşağıda belirtilen amaçlar doğrultusunda tasarlanır. Şekil 14.2'de bu yapı verilmiştir. Bu yapı içerisinde,

-merkezi bir izleme noktası sağlanması, tehditlerin sentezlenmesi ve bu tehditler doğrultusunda harekete geçilmesi

- Siber olaylara karşı hazırlık ve müdahale

- İş sürekliliğine ve verimli kurtarmaya olanak sağlanması

- Siber tehditlerin iş altyapısını etkilemesinin önlenmesi

- İçgörüler sunan siber risk ve uyumluluk raporlaması sağlanması

- Risklerin hızla ortadan kaldırılması için güvenlik duvarları, izinsiz giriş önleme sistemleri ve yönlendiriciler gibi kritik altyapı bileşenlerini yöneten grupların potansiyel tehditlerden haberdar olmasının sağlanması

Daha ayrıntılı bir biçimde ifade etmek gerekirse, kurumsal güvenlik operasyon merkezinin başlıca sorumlulukları aşağıda belirtilen konularda yardımcı olmaktır:

- İzinsiz giriş olaylarının izlenmesi, analiz edilmesi, ilişkilendirilmesi ve üst kademelere iletilmesi

- Güvenlik tehditlerindeki eğilimlerin ve bunların işletme üzerindeki potansiyel etkisinin belirlenmesi
- Koruma, savunma ve müdahale için uygun tepkilerin geliştirilmesi
- Güvenlik olayı yönetimi ve adli soruşturma gerçekleştirilmesi
- Güvenlik topluluğu ile ilişkilerin sürdürülmesi
- Kriz operasyonlarına ve iletişimlerine destek sağlanması

Şekil 14.2. Güvenlik Operasyon Merkezlerinde tek gösterim

Bunlar, genel olarak kuruluşlar için kritik önem taşıyan BT güvenliği işlevleridir, ancak bunların bir kurumsal güvenlik operasyon merkezi aracılığıyla yönetilmesi, özellikle katı hukuki ve uyumlulukla ilgili gereksinimlere tabi olan ve ele geçirilmesi durumunda yıkıcı sonuçlar doğurabilecek yüksek hacimli hassas verilerle uğraşan şirketler için avantajlı olabilir. Buna bağlı olarak bir kurumsal güvenlik operasyon merkezi, özellikle finans kuruluşları, büyük ilaç şirketleri ve devlet kurumları için uygun bir çözümdür. Küçük ve orta ölçekli işletmelerin aksine, daha büyük kuruluşlar, kurumsal bir güvenlik operasyon merkezinin oluşturulup yönetilmesi ve

24 saat izleme yeteneğinin geliştirilmesi için gerekli olan insan kaynaklarını, teknolojileri ve fiziksel alanı daha kolay tahsis edebilirler.

Her kurumsal güvenlik operasyon merkezinin ait olduğu kuruluş kadar özgün olması nedeniyle, sonucu etkileyen faktörlerin anlaşılması kritik önem taşır. Bir kurumsal güvenlik operasyon merkezi, tamamen dahili operasyonlardan, süreçlerden, teknolojiden ve personelden oluşabilir, önemli ölçüde harici sağlayıcıların yönetilen hizmetlerine bağımlı olabilir ya da dışarıdan temin edilen yeteneklerle dahili yeteneklerin bir bileşimini içerebilir. Kuruluşunuz için doğru dengeyi belirlemek amacıyla maliyeti, becerilerin mevcut olup olmadığını, çok sayıda küresel lokasyona karşılık tek noktadan faaliyet göstermeyi, 24 saat çalışmanın ve desteğin önemini değerlendirmek isteyebilirsiniz.

Hangi modeli tercih ederseniz edin, kurumsal bir güvenlik operasyon merkezi genel olarak aşağıda belirtilen avantajları sağlayabilir:

- Kişiler, süreçler ve teknolojiler tarafından desteklenen ve güvenlik olaylarını daha etkili bir biçimde önleyen, azaltan ve çözen, 24 saat etkin bir operasyon yapısı
- Başka şekilde manuel keşif ve ilişkilendirme gerektirecek olan siber saldırılara, virüslere ve kötü amaçlı kullanıma ilişkin iyileştirilmiş görünürlük
- Güvenlik programınızın operasyon risklerini ve buna bağlı olarak iş risklerini nasıl azalttığına ilişkin daha iyi bir anlayış
- Giderek artan uyumluluk gereksinimlerinin karşılanmasına yardımcı olması için iyileştirilmiş analitik ve raporlama
- Güvenlik yapınızın mevcut durumuna ilişkin içgörü
- Harici hizmet sağlayıcıların tehdit akışları ve analitiği aracılığıyla olanak sağlanan daha kapsamlı bir tehdit görünümü
- İşletmenizin değişen risk yönetimi gereksinimlerinin karşılanması için güvenlik teknolojilerinizin güncellenmesinde daha fazla esneklik
- Kuruluşunuzun en değerli varlıklarından biri olan bilgilerinizi yönetmenize yardımcı olması için tehdit denetiminin daha iyi merkezileştirilmesi

- Güvenlik tehditlerinin önlenmesine ve etkisinin azaltılmasına yardımcı olarak maliyetlerin ve işletme markasının uğrayabileceği zararın azaltılması

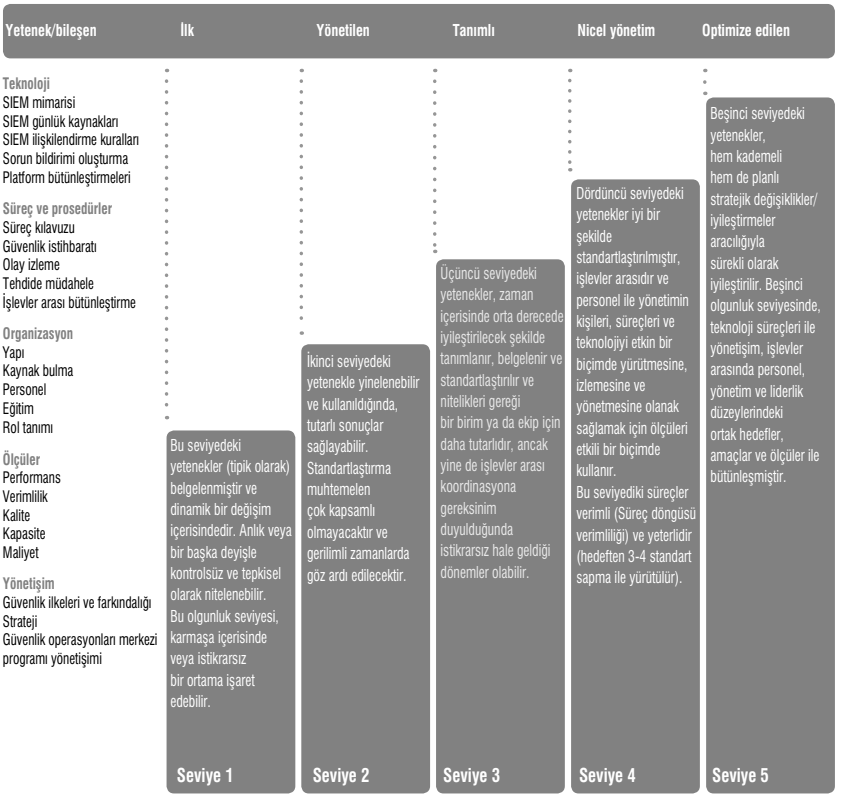
14.4. Mevcut Güvenlik Operasyonlarının Değerlendirilmesi

Hemen her kuruluşun birtakım güvenlik operasyonları vardır ve hatta çoğu kuruluş, özel olarak tahsis edilmiş güvenlik operasyon merkezleri oluşturmuştur. Ancak, bunlar genellikle optimum düzeyin altında faaliyet gösterirler ve gerekli tehdit koruması düzeyini sağlamazlar. Bazı durumlarda güvenlik operasyonları, tehdit izlemenin ağ aygıtları için ilke yönetimi süreçleri ile bağlantılı hale getirilmesi amacıyla ağ operasyon merkezine entegre edilir. Buradaki risk, grubun yönetişim önceliklerinin tehditleri belirlemeye ve analiz etmeye yeterince ağırlık vermemesi olabilir. Ayrıca, odak noktası ağın yönetilmesi olduğundan, ağ bağlamının dışındaki tehditler konusunda boşluklar ortaya çıkabilir. Özel olarak tahsis edilmiş bir güvenlik operasyon merkezi, tehditlerin hem operasyon bakımından hem de planlama bakımından işletmeyi nasıl etkileyebileceğine öncelik verebilir. Bu ayrıca, kuruluşun, tehditlerin gelişen yapısına ve işletmeyi nasıl etkilediğine ilişkin bilgileri daha kolay paylaşabilecek becerikli analistlerden oluşan bir ekibi bir araya getirmesine yardımcı olur.

Mevcut operasyonun değerlendirilmesinde göz önüne alınacak önemli noktalardan biri, mevcut olgunluk düzeyidir. Mevcut operasyonların olgunluğu, kuruluşun korunması için gerekli olan tehdit yönetimi yeteneklerinin sağlanmasındaki etkinliğin bir ölçüsüdür. Olgunluk düzeyleri, artan olgunluk ölçeği doğrultusunda çok sayıda yetenek veya bileşen boyutu esas alınarak değerlendirilmelidir. Ölçülecek yetenekler veya bileşenler arasında aşağıda belirtilenler yer alabilir:

- Teknoloji
- Süreç ve prosedürler
- Organizasyon
- Ölçüler ve
- Yönetişim

Bu alanların her birinin incelenmesi yoluyla, bunları ilk temel yeteneklerden optimize edilmiş bir ortama kadar, beş tanım genelinde derecelendirerek mevcut yapının sektördeki en iyi uygulamalara göre durumunu belirleyebilirsiniz, Şekil 14.3'te bu derecelendirme gösterilmektedir. Bu alanlardan herhangi birindeki düşük bir derecelendirme, yönetimin daha fazla ilgi göstermesi ve yatırım yapması gerektiğini gösterir. Benzer şekilde, yetenekler ya da bileşenler arasındaki bir uyumsuzluk (birinin düşük, diğerinin yüksek olması), yatırım kaynaklarınını verimsiz bir biçimde tahsis edildiğini ifade edebilir.



Şekil 14.3. Güvenlik operasyonlarının olgunluk seviyelerinin değerlendirilmesi

14.5. Kurumsal Bir Güvenlik Operasyon Merkezinin Beş Temel İşlevi

Kurumsal bir güvenlik operasyon merkezinin avantajlarını gerçeğe dönüştürmeniz, temel kurumsal güvenlik operasyon merkezi işlev-

lerine yönelik stratejiyi ne kadar etkili bir biçimde tanımladığınıza bağlıdır. Bu beş temel işlev Şekil 14.4'de belirtilen işlevlerden oluşur:

- Güvenlik tehditlerinin izlenmesi
- Güvenlik olayı yönetimi
- Personelin işe alınması, elde tutulması ve yönetilmesi
- Süreçlerin geliştirilmesi, yönetilmesi ve optimizasyonu
- Yükselen tehdit stratejisi

Şekil 14.4. Güvenlik operasyon merkezinin beş temel işlevi

14.5.1. Birinci İşlev: Güvenlik Tehditlerinin İzlenmesi

Tehdit verilerinin izlenmesi ve olası güvenlik olaylarının nerede soruşturulması gerektiğinin belirlenmesi, güvenlik tehditlerinin ortaya çıkmadan önlenmesinin en iyi yollarından biridir. Güvenlik

bilgisi ve olay yönetimi (SIEM) sistemi teknolojileri ve diğer araçlar gibi güçlü izleme becerilerinin ve kaynaklarının mevcut olması, kuruluşunuzun güvenlik olaylarına tepki veren yapısını, bu olayları en baştan önleyen bir yapıya dönüştürmenize olanak sağlayabilir.

SIEM araçları, kurumsal güvenlik operasyon merkezi için, tehditlerin belirlenmesine, ilişkilendirilmesine ve öncelikli hale getirilmesine olanak sunan teknoloji temelini sağlar. Daha iyi bir görünürlüğe imkan tanıyan SIEM teknolojileri; İzinsiz Girişi Önleme Sistemleri (IPS), güvenlik duvarları, yönlendiriciler gibi çok sayıda aygıt çapındaki yüksek hacimli günlük verilerini toplar ve bu verileri eyleme dönüştürülebilir güvenlik istihbaratı haline getirir. Bu özellik, milyarlarca günlük olayının sentezlenerek düzeltme eylemi için öncelikli hale getirilebilecek az sayıda güvenlik ihlaline indirgenmesine yardımcı olur.

Ancak güvenlik olaylarının başarıyla önlenmesi, yalnızca sektör lideri teknolojiye değil aynı zamanda sektör lideri stratejiye de bağlıdır. Aşağıda belirtilenleri göz önünde bulundurmak gerekecektir.

14.5.1.1. Metodoloji

- Hangi belirli verilerin izlenmesi gerekiyor ve bunların belirli saatler içerisinde mi yoksa 24 saat mi izlenmesi gerekiyor?
- Hangi güvenlik olaylarını izleyeceksiniz ve bu olayları izleme teknolojisi için kurallar aracılığıyla nasıl tanımlayacaksınız?
- Belirli verilerin izlenmesini gerektiren uyumluluk ve yasal düzenleme sorunları neler?
- İzlediğiniz sistemler iş sürekliliği ve olağanüstü durum kurtarma planınıza dahil edilmek için yeterince kritik mi?

14.5.1.2. Kaynaklar

- Hangi tür izleme raporları gerekli olacak ve bu bilgiler kimler tarafından tüketilecek?
- En yeni tehditlerden korunmak için hangi SIEM yetenekleri gerekli olacak?
- İzleme için hangi insan kaynakları gerekli ve kaç kişi gerekli?
- İş gereksinimlerini en iyi şekilde karşılayacak nitelikler hangileri?

14.5.1.3. Ekip Katılımı

- Ekibinizin motivasyonunu ve eğitimini nasıl sürdürebilirsiniz?
- Ekibiniz etkili karar alma için doğru miktarda bilgiye sahip mi?
- Yeni çalışanları nasıl eğiteceksiniz?

14.5.1.4. Takip

- Bir güvenlik olayının soruşturulması gerektiğinde üst kademeye iletme süreciniz nasıl olacak? Üst kademeye iletilen olaylar nasıl soruşturulacak?
- Sürekli süreç iyileştirmeyi izleme sürecine nasıl bütünleştireceksiniz?
- Kullanım senaryolarının en son tehdit kalıplarını temsil etmesini nasıl sağlayacaksınız?
- İzleme araçlarına akışları duran günlük ve olay kaynaklarını nasıl saptayacaksınız ve düzelteceksiniz?
- Teknoloji ve tehditler değiştikçe izleme yeteneklerinizi hakkında kuruluşunuzu nasıl bilgilendireceksiniz?

Listenin tamamı bunlarla sınırlı olmamakla birlikte, bunlar bir SIEM sisteminin ya da diğer izleme araçlarının seçilmesinin ötesinde göz önünde bulundurulması gereken kritik öğelerdir. Ayrıca, bu sorulara verdiğiniz yanıtların çoğu, yalnızca kullandığınız izleme teknolojisini belirlemenize yardımcı olmakla kalmayacak, aynı zamanda güvenlik izleme operasyonlarınızı yürüten kişi ve teknolojileri ne kadar etkili bir biçimde optimize edebileceğinizi de belirleyecektir.

14.5.2. İkinci İşlev: Güvenlik Olayı Yönetimi

Güvenlik tehditlerinin belirlenmesi yalnızca ilk adımdır. Hangi güvenlik olaylarının müdahale gerektirdiğinin ve riskin ortadan kaldırılması için gerekli eylemlerin gerçekleştirilmesinin nasıl sağlanacağının belirlenmesi de aynı ölçüde önemlidir. Bütünleşik bir sorun bildirimi sistemi, tehdit analizinin yakalanması, bir güvenlik olayı olarak işlenmesi ve gerekli düzeltici eylemlerin gerçekleştirildiğinin takip edilmesi için gerekli olan mekanizmayı sağlayabilir. Bu yaklaşım, ilke değişiklikleri gerektiren aygıtları yöneten ekiplerle bağlantı kurulmasını kapsar. Çoğu güvenlik aygıtı tipik olarak

güvenlik operasyon merkezinin dışında yönetildiğinden, risk altındaki aygıtın ve sorumlu tarafların hızla belirlenmesi, kuruluşların tehdide karşı ilkeleri ve yapılandırmaları daha hızlı güncellemesine olanak sağlar.

Güvenlik olaylarının yönetilmesine ilişkin bazı uygulanabilir noktalar arasında aşağıda belirtilenler sayılabilir:

- Güvenlik olaylarının yönetilmesi için öncelik verme süreci (Önem Düzeyi 1–3)
- Bildirim sürecinin tanımlanması (kim ve ne zaman)
- İş yükünün ve sorun bildirimlerinin eskimesinin yönetilmesi
- Hizmet seviyelerinin tanımlanması ve uygulanması
- Performansın takip edilmesi için anlamlı ölçüler geliştirilmesi

Ayrıca, aygıtlarla ve ilkelerle ilgili olarak göz önüne alınması gereken noktalar da bulunur. Bunlar arasında aşağıda belirtilenler yer alır:

- Güvenlik aygıtlarının ve araçlarının ilkeleri nasıl oluşturulacak ve test edilecek?
- Değişiklikler nasıl uygulanacak, değişiklikleri yapmak için kim yetkili olacak ve yetki nasıl verilecek? Genel ilkeleri kim düzenli olarak inceleyecek?
- Güvenlik tanımı dosyalarını nasıl güncelleyeceksiniz?
- Engelleme teknolojileri uygulayacak mısınız ve uygulayacaksanız, hangi öğeler için?
- Sağlıklı işletim durumu ve kullanılabilirlik için aygıtları nasıl izleyeceksiniz?
- Sağlıklı işletim durumunun izlenmesine ilişkin bilgilendirmeleri hangi ekipler alacak?
- Sağlıklı işletim ve ilke sorunlarını nasıl güncelleyecek, kaydedecek ve takip edeceksiniz?
- Yazılımlar ve sabit yazılımlar nasıl güncellenecek?
- Ağ geçidi aygıtları ile yerleşik aygıtlar için hangi ölçüde hata toleransı gerekli olacak?

- Aygıtlara erişim yetkisini nasıl vereceksiniz ve değişiklikler nasıl izlenecek?
- Üçüncü kişiler için erişim nasıl denetlenecek?
- Değişiklikler ve ayarlamalar için izleme ekibi ile aygıt ve ilke ekibi arasındaki geri bildirim süreci nasıl olmalı?

14.5.3. Üçüncü İşlev: Personelin İşe Alınması, Elde Tutulması ve Yönetilmesi

Güvenlik olaylarını sürekli olarak izlemesi ve bu olaylara müdahale etmesi için işe aldığınız kişiler, kurumsal güvenlik operasyon merkezinizin temelini oluşturacaktır. Bu nedenle, onları akıllıca seçmeniz gerekir. Başlangıç seviyesinde niteliklere sahip personeli işe almak ve eğitmek size kısa vadede tasarruf sağlayacak olsa da, güvenlik tehditlerini etkin biçimde analiz etme, ortaya çıkmadan önleme ya da çözme becerilerine sahip olmamaları durumunda bu strateji uzun vadede geri tepebilir.

Tehditlerin filtrelenmesi ve en önemli risklerin belirlenmesi SIEM tarafından yerine getirilecek olsa da, insan bileşeni halen kritik önem taşımaktadır. Her gün BT tehditlerini bertaraf etmek çok büyük bir konsantrasyon, ayrıntılara dikkat ve en önemlisi de önemli ölçüde analitik becerileri gerektirir. Ağ ve masaüstü desteği ile sorun giderme becerileri, bu alanda genellikle yararlı olabilir. Ayrıca, ortamda kullanılan satıcı firma teknolojisine ilişkin bir miktar uzmanlığa sahip olunması da önemlidir.

Ekiplerin aynı zamanda, güvenlik istihbaratını kullanmaya ve en son uyarıların kuruluş için yeni bir tehdit düzeyine işaret edebileceğini belirlemeye yönelik yaklaşımlarında proaktif olması gerekir ve bu da analistler arasında yakın iş birliğini ve bilgi paylaşımını gerektirir.

Buna ek olarak, kaynak tahsisini potansiyel tehdit hacmi ve etkisi ile eşleştiren bir vardiya planlama programına sahip olmanız gerekecektir. Bu, tüm dünyaya yayılmış çok sayıda kurumsal güvenlik operasyon merkezi bulunan büyük kuruluşlar için kaynakların "follow-the-sun" yaklaşımıyla dağıtılmasını gerektirebilir.

Ayrıca, eğitimin taşıdığı kritik önemi de unutmayın. Hem güvenlik teknolojileri, hem de tehdit ortamı sürekli olarak değişirken, resmi bir program aracılığıyla sürekli eğitim bir zorunluluktur.

Personele ilişkin olarak göz önünde bulundurulması gereken diğer noktalar aşağıda belirtilmiştir:

- Her personel için iş gereksinimlerini esas alan vardiya planları (örneğin, Pazartesi ile Cuma arası, 08.00 ile 17.00 saatleri arasında ya da 24 saat)
- Her pozisyon ve her planlı vardiya için tanımlanmış sorumluluklar ve teslim edilecek malzemeler
- Güvenlik izleme ve teknoloji yönetimi becerileri (Not: UNIX ve Linux becerileri güvenlik alanında genellikle yararlıdır)
- SANS gibi eğitim organizasyonları ve yenilikçi güvenlik eğilimlerinin ele alındığı Black Hat Toplantılar ile güvenlik konferansları gibi etkinliklere katılım için göz önüne alınması gereken bütçe hususları
- Güvenlik profesyonelleri için kariyer rotası; pozisyonun zorlukları nedeniyle kurumsal güvenlik operasyon merkezi analistleri için tipik çalışma süresi 1 ile 3 yıl arasıdır
- Sürekli istihdam stratejileri
- İzleme aracı için yeni kuralların yazılmasına odaklanan, genellikle yalnızca derin güvenlik uzmanlığı değil aynı zamanda komut dosyası yazma uzmanlığı da gerektiren özel pozisyonlar

Aynı zamanda, erişimin anlaşılması ve harici güvenlik hizmeti sağlayıcılar dahil olmak üzere güvenlik ekibindekilere sağlanan erişimin denetlenebilmesi de önemlidir. Bunun nedeni, bu ekiplerin ayrıcalıklı bilgilere ve kritik dahili sistemlere yönelik sistem yöneticisi kimlik bilgilerine erişime sahip olma olasılıklarıdır.

14.5.4. Dördüncü İşlev: Süreçlerin Geliştirilmesi, Yönetilmesi ve Optimizasyonu

Kurumsal bir güvenlik operasyon merkezinin etkin biçimde yönetilmesi, iyi tanımlanmış süreçler ve prosedürler gerektirir. Belirli bir görevin kim tarafından yerine getirileceği bir süreç tarafından belirlense de, görevin fiilen nasıl yerine getirileceği bir prosedür tarafından belirlenir. Sürekli olarak düzenli, verimli ve yüksek düzeyde tutarlı bir şekilde faaliyet gösterilmesi için her ikisi de gereklidir. Bunlar, ekiplerin görevlerini nasıl yerine getireceklerini bilmelerine yardımcı olur.

Kurumsal güvenlik operasyon merkezi sürecine ilişkin olarak göz önünde bulundurulması gereken sayısız nokta arasında aşağıda belirtilenler yer alır:

- Güvenlik sorunlarının belirlenmesi ve çözülmesi için analitik süreçleri ve prosedürleri

- Güvenlik olayı sınıflandırma metodolojisi
- Güvenlik olayı saptama ve harekete geçilmesi için analitik zaman çizelgeleri
- Güvenlik olaylarını üst kademeye iletme süreci ve takip
- Güvenlik olaylarının analistlere yönlendirilmesinin ve çözülmesinin sağlanmasına yardımcı olması için sorun bildirimi
- Yeni tehditlerin değerlendirilmesine yönelik süreç
- Yeni saptama kurallarının yazılmasına ve test edilmesine yönelik süreç
- Adli soruşturma süreçleri

- Sistem yönetimi görevleri ile idari görevler için iş süreçleri ve prosedürleri

- Günlüklerin saklanması
- Kabul edilebilir olmayan kullanım
- Dahili iletişimler ve kamunun bilgilendirilmesi
- Ağ geçidi aygıtlarındaki değişiklikler ve bu yapılandırmaların nasıl inceleneceği dahil olmak üzere ilke değişiklik süreci ve doğrulaması
- İçerik güncelleme süreci ve kullanım senaryosu yenilemeleri
- Rapor hazırlama ve ölçü raporlaması

- Günlük operasyonlar için operasyonel süreçler ve prosedürler

- Personelin işe alınması, elde tutulması, terfisi ve devri
- Yeni personelin işe alıştırılması
- Şirket güvenlik farkındalığı eğitimi
- Personel eğitimi

- Sistem yönetimi, bakım ve idare için teknoloji süreçleri

- Yama süreci
- Sabit yazılım güncelleme süreci ve yazılım güncellemeleri
- Aygıt ve yönetim istasyonu süreçlerine erişim
- Yeni teknoloji uygulama süreci
- Sağlıklı işletim denetimi süreci
- Güvenlik açığı taraması ve düzeltme süreci

Bu daha geniş kategorilerin her biri yüzlerce ayrıntılı prosedüre bölünebilir. Süreçlerinizi planlamada ne kadar titiz olursanız, kurumsal güvenlik operasyon merkeziniz o kadar etkili olur.

14.5.5. Beşinci İşlev: Yükselen Tehdit Stratejisi

En yeni güvenlik istihbaratına erişimleri olmadığında kuruluşlar, bir tehdidin mevcut olduğundan habersiz bir şekilde en kritik iş verilerini bilgisayar korsanlarının veya kötü niyetli yazılımların erişimine açık halde bırakabilirler. Ancak bu gerçeğe rağmen, çoğu şirket en yeni güvenlik istihbaratına erişememektedir.

Bu, genellikle güvenlik istihbaratının hızla değişmesinden ve bunun da güncel ve yükselen tehditlere ayak uydurmayı zorlaştırmasından kaynaklanır. Ancak, hizmet olarak edinilebilecek tehdit analizi gibi tehdit hizmetlerine abonelikler ve benzeri pek çok kaynak mevcuttur.

Ayrıca, harici IP adreslerinin güvenilirliğini sınıflandırabilen ve kendi adres alanınızın bilinen botnet kontrol istasyonlarıyla iletişim kurması halinde sizi uyaran hizmetlere abone olmak da mümkündür.

Buna ek olarak, kuruluşunuzu etkileyen tehditlerin ve olayların benzer şirketlerin karşı karşıya olduklarıyla aynı düzeyde olup olmadığını anlamak yararlıdır. Bu içgörü, ne bekleyebileceğinizi, savunma mekanizmalarınızın ne kadar etkili olduğunu ve güvenlik programınızın etkinliğini değerlendirmenize yardımcı olabilir. Kuruluşunuz ve süreçleriniz de, bu güvenlik istihbaratından yararlanmak ve risk vektörleri değiştikçe kaynakları ve öncelikleri yeniden yönlendirmek için gereken çevikliğe sahip olmalıdır.

İdeal olarak aşağıda belirtilenler içeren belirli güvenlik ölçüleri oluşturmanız gerekecektir:

- Gün başına ve tür başına olaylar için yaygın tehdit tabanı ölçüleriniz olarak kullanılmaya uygun bir dizi ölçü
- İş denetimi gereksinimlerini karşılayabilen uyumluluk raporları
- Genel şirket ölçülerinize ve iş hedeflerinize daha iyi uyum sağlayan güvenlik raporlaması

Mutasyona uğrayan tehditlerin farkında değilseniz, bunları başarıyla yönetemezsiniz. Buna bağlı olarak, tehdit ortamının sürekli olarak taranması, güvenlik izleme çabalarınızı daha etkili hale getirebilir.

14.6. Kapasite yönetimi

Kapasite yönetimi, güvenlik operasyon merkezinin boyutlandırmasının öngörülen tehditlerin türü ile hacmine ve korunacak altyapının genişliğine uyarlanmasında önemli bir rol oynar. Daha önce açıklanan olgunluk analizinde olduğu gibi, aşırı yatırım yapılmaksızın azami hacim gereksinimlerinin karşılanması için güvenlik operasyon merkezinin çeşitli öğelerinin (kişiler, süreçler ve teknoloji) dengeli ve yeterli olması önemlidir. Ayrıca, bunların tipik olarak hizmet seviyesi sözleşmelerinde ve hizmet seviyesi hedeflerinde tanımlanan performans seviyelerine ulaşılmasını sağlayacak şekilde boyutlandırılması gerekir.

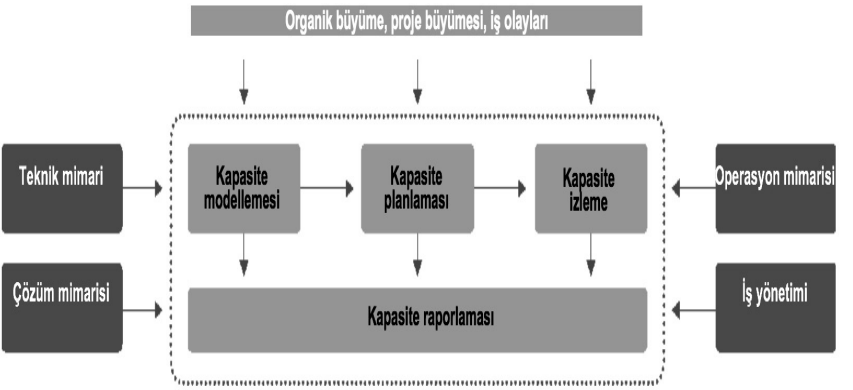
Kapasite yönetimi, Şekil 14.5'te gösterdiliği gibi birbirinden ayrı dört aşama olarak düşünülebilir :

i. Kapasite modellemesi

Beklenen iş yükünü karşılayabilecek doğru kaynak dengesini sağlayacak etkili bir iş hacmi kapasitesi elde edilmesi için tasarım kapasitesinin ne olması gerektiğinin anlaşılması amacıyla güvenlik operasyon merkezinin girdi ve çıktılarının analiz edilmesidir. Gerekli olan farklı becerilere, teknoloji iş hacmine, hizmetin sağlanması gereken saatlere ve benzeri hususlara olanak sağlanması için bir dizi modelleme aracı kullanılabilir. Bu, basit kuyruklama teorisinden Erlang modellemesine ve Poisson dağıtımlarının geliştirilmesine kadar uzanabilir. Bu çalışma, gerekli olan kaynak düzeyine ve bunların tahsisine ilişkin nicel bir görünüm sağlar.

ii. Kapasite planlaması

Modelleme çalışması, güvenlik operasyon merkezi faaliyetlerinin ve bileşenlerinin boyutlandırılması ve kapsamının belirlenmesi için gerekli olan girdileri sağlar. Bu, tanımlı vardiyalar için gerekli olan becerilerin sayısına ve türüne, analitik ve güvenlik olayı işleme süreçlerinin desteklenmesi için gerekli olan sunucu sayısına ve kapasitesine, gereksinimlerin desteklenmesi için gerekli olan yatırıma ve bütçenin hazırlanmasına ilişkin kararların daha bilgili bir biçimde alınmasına imkan tanır. Planlama aşaması, tipik olarak üç yıllık bir güvenlik operasyon merkezi stratejisi ve planı ile sonuçlanır ve bunlar daha sonra iş gereksinimlerindeki ya da tehdit ortamındaki değişikliklere bağlı olarak güncellenir. Bu planlama, tipik olarak hem iş hem de BT ve uyumluluk birimlerinden paydaşların katılımıyla gerçekleştirilir.



Şekil 14.5. Kapasite yönetimi, tipik olarak dört ayrı aşamaya ayrılır.

iii. Kapasite izleme

Modelleme çalışmasında alınan kararların doğrulanması için güvenlik operasyon merkezi performansının düzenli olarak değerlendirilmesi önemlidir. Daha önce belirtilmiş olduğu gibi, günümüzün tehdit ortamı sürekli olarak değişmekte ve personelin düzenli olarak yeniden dengelenmesini ya da mevcut becerilerin gözden geçirilmesini gerektirebilmektedir. Buna bağlı olarak, yönetime güvenlik operasyon merkezinin tanımlanmış misyonunu yerine getirip getirmediğinin değerlendirilmesi için gerekli olan araçları ve bilgileri sağlayan izleme yeteneklerinin mevcut olması önem taşır. Bu, yalnızca mevcut operasyonun gerekçelerini teyit etmeye yar-

dımcı olmakla kalmaz, aynı zamanda gelecekteki gereksinimlere, örneğin, iyileştirilmiş güvenlik istihbaratı işleme teknolojilerine ya da geliştirilmiş raporlama yeteneklerine duyulacak gereksinimlere ilişkin öngörüler de sağlar.

iv. Kapasite raporlaması

Yukarıda belirtilen aşamaların desteklenmesi, güvenlik operasyon merkezi yönetimine yalnızca mevcut operasyonun performansının ve hizmet seviyesi sözleşmeleri ile hizmet seviyesi hedeflerinin karşılanıp karşılanmadığının değerlendirilmesi için değil, aynı zamanda süreç, beceri ya da teknoloji kısıtlamalarının hacimdeki bir artışın ya da iş hedeflerindeki bir değişimin karşılanmasını nerede engelleyebileceğinin daha iyi anlaşılması için gerekli olan bilgileri sağlayan kapsamlı raporlama için gereklidir. Etkili raporlama, hem güvenlik operasyon merkezi yöneticileri ile üst düzey bilgi güvenliği yöneticisinin hem de kuruluşun bilgi gereksinimlerini karşılar. Aynı zamanda, hazırlığın kanıtlanmasına ve güvenlik operasyon merkezi geliştikçe gelecekteki yatırım taleplerinin desteklenmesine yardımcı olması için uyumluluk raporlaması sağlayabilir.

14.7. Değerlendirmeler

Siber güvenlik operasyon merkezini anlamak için, "Kurumsal bir güvenlik operayon merkezi nasıl kurulur?", "Bir güvenlik operasyon merkezi girişimi nasıl başlatabilir?" gibi sorulara net cevap verilmeli ve bu hususlar ise detaylı değerlendirilmelidir.

Pratik bir başlangıç noktası, kuruluşun risk yönetimi hedeflerinin anlaşılmasıdır. Bunun için aşağıdaki sorulara cevaplar bulunmalıdır.

- İş yönetiminin zaman ayırdığı ve yatırım sermayesini yönlendireceği iş riskleri ya da uyumluluk gereksinimleri nelerdir?
- Güvenlik operasyon merkezi stratejisine girdi sağlamak isteyecek önemli iş ve BT paydaşları kimlerdir?

Bu sorular ile bunlara verilecek olan yanıtlar, misyon beyanınızı geliştirmenize yardımcı olacaktır. Kurumsal bir güvenlik operasyon merkezinin misyonu, bu merkezi oluşturma gerekçenizi ve aşmayı hedeflediği sorunları kapsamalıdır. Bu misyon, kuruluşunuza özgü olacaktır ve kurumsal güvenlik operasyon merkezinizi oluşturacak

kişilerin, süreçlerin ve teknolojilerin belirlenmesine yardımcı olacaktır.

Örnek olarak; finansal bir kuruluşta bir güvenlik operayon merkezi kurmak için strateji danışmanlığı ve uygulama desteği alınmalıdır.

Senaryo:

Tüm dünyaya yayılmış çok sayıda lokasyonu bulunan küresel bir finans kuruluşu, şirket içinde tehdit yönetimini iyileştirmelerine ve uyumluluğu daha iyi yönetmelerine yardımcı olacak kurumsal bir güvenlik operasyon merkezi yaratmak için sektör lideri güvenlik uygulamalarına ilişkin içgörülere ve desteğe gereksinim duyar.

Aranan çözüm:

- Mevcut güvenlik operasyonlarının değerlendirilmesi için iş çalıştayları ve teknik çalıştaylar
- Önde gelen SIEM teknolojilerinden yararlanan, sınıfının en iyisi güvenlik operasyon merkezinin oluşturulmasına yönelik danışmanlık
- 24 saat çalışan bir güvenlik operasyon merkezi oluşturulması için uygulama ve bütünleştirme hizmetleri ve operasyonun hızla faal hale getirilmesine yardımcı olması amacıyla personel desteği

Avantajları:

- Mevcut olgunluğun ve mevcut güvenlik operasyonlarının yeteneklerinin bir görünümü
- Daha düşük maliyetler ve daha yüksek yatırım getirisi
- Tehditlerin izlenmesi ve yönetilmesi için optimize edilmiş süreçler
- Değişen uyumluluk gereksinimlerine hızla yanıt verme becerisi
- Tehditlere ilişkin daha iyi görünürlük ve risklerin daha iyi giderilmesi

Misyonu oluştururken aşağıdaki konular gözönünde bulundurulmalıdır:

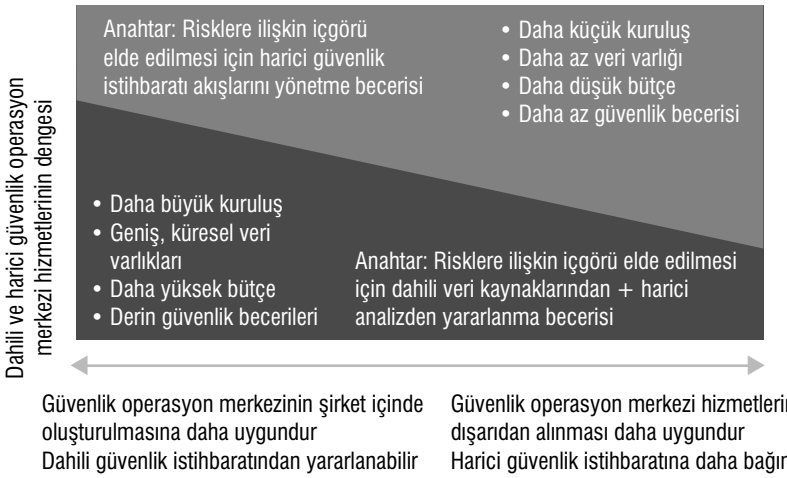
- Tanımlanmış iş ve BT risklerine dayalı olarak sorunlu güvenlik noktaları

- Sorunlu noktalarınızı etkin bir biçimde karşılayacak temel kurumsal güvenlik operasyon merkezi işlevleri
- Özellikle diğer coğrafi bölgelerde olabilecek birimler için uyumluluk ve yasal düzenleme gereksinimleri
- Güvenlik bütçesi ve birkaç yılı kapsayan bağlılık
- Bugüne kadar karşı karşıya kalmış olduğunuz tehditlerin hacmi ve türleri
- Kurumsal güvenlik operasyon merkezi tarafından toplanan ve analiz edilen bilgileri kimin tüketeceği
- Tesisler
- Emek ve beceri kullanılabilirliği
- Mevcut ve gerekli teknolojiler
- Eğitim ve tehdit istihbaratı eğitsel yatırımları

Hedeflerinizi tanımladıktan sonra, nelerin işe yaradığını ve nelerin işe yaramadığını belirlemek için bunları mevcut güvenlik durumunuzla karşılaştırın. Örneğin, güvenlik aygıtlarınızın günlük raporlarına ilişkin tam görünürlüğe sahip misiniz? Kullanışlı güvenlik istihbaratı elde etmek için günlük bilgilerini ilişkilendirebiliyor musunuz? Güvenlik yönetişiminiz belirlenen tehditlere hızla müdahale edilmesinin sağlanmasına yardımcı oluyor mu? Güvenlik operasyonlarınızın değerlendirilmesi, personel, süreçler veya teknolojiler bakımından mevcut olabilecek ve bir ihlale kapı açabilecek eksiklikleri belirleyebilir. Aynı zamanda, devam etmek için gereksinim duyacağınız kaynakların ve yeteneklerin daha net bir resmini çizebilir. Bu içgörülerle, misyon beyanınızda ve hedeflerinizde ince ayarlamalar yapabilir ve en sonunda, bunları kurumsal güvenlik operasyon merkezi faaliyetlerinizin oluşturulması için bir yol haritasına dönüştürebilirsiniz.

Son olarak, iş yükünün ve sermaye yatırımlarının ne kadarını şirket içinde gerçekleştireceğinizi belirlemeniz gerekecektir. Devam etmek için, bir yönetilen güvenlik hizmetleri sağlayıcısının becerilerinden yararlanılması, stratejinin ve kurumsal güvenlik operasyon merkezinin tamamen şirket içinde oluşturulması ya da temel işlevlerden bazıları için dış kaynak sağlamadan yararlanılması dahil olmak üzere çeşitli seçenekler bulunur. Örneğin, SIEM teknolojisini

yönetmesi ya da size sözleşme kapsamında uzman analist kaynakları sağlaması için bir hizmet sağlayıcı seçebilirsiniz. Şekil 14.6'da, kurumsal güvenlik operasyon merkeziniz için optimize edilmiş bir model belirlenmesinde rol oynayan faktörler gösterilmektedir.



Şekil 14.6. Güvenlik operasyon merkeziniz için uygun seçeneğin belirlenmesi

Güvenliğe ilişkin tüm sorumluluğu dış kaynak sağlayıcılara devredebilecek şirketler çok azdır ya da hiç yoktur. Ancak pek çok kuruluş, bir güvenlik hizmetleri sağlayıcısı ile iş birliği yapmanın bu belgede ele alınan temel işlevleri daha etkili ve verimli bir biçimde yerine getirmelerine yardımcı olabileceğini görmüştür. Bunun nedeni, güvenlik operasyonlarının yoğun olabilmesi, çok sayıda hususun göz önüne alınmasını ve geniş bir beceri yelpazesini gerektirmesidir. Geniş güvenlik kaynaklarına sahip olan bir sağlayıcı, aşağıda belirtilen hizmetlerden birini ya da daha fazlasını sağlayarak kurumsal güvenlik operasyon merkezinizin geliştirilmesini hızlandırabilir:

- Strateji danışmanlığı ve kurumsal güvenlik operasyon merkezi tasarım ve uygulama uzmanlığı
- Birinci sınıf beceriler
- Uyumluluk ve yasal düzenleme yönetimi
- Gelişmekte olan tehditlerin belirlenmesi için kapsamlı güvenlik araştırması

- Güvenlik tehditlerinin izlenmesine, çözülmesine ve önlenmesine yardımcı olan birinci sınıf teknolojiler

Kaynaklar

[1] Gartner, "Forecast: Information Security, Worldwide, 2011-2017, 3Q13 Update," Ekim 2013. #G00258387

[2] IBM, "IBM Security Services Cyber Security Intelligence Index," Mart 2013, ibm.com/services/multimedia/Cyber_security_Index.pdf

[3] Ponemon Institute, "2013 Cost of Data Breach Study:Global Analysis," Mayıs 2013; https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_ Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[4] Ponemon Institute: "Reputation Impact of a Data Breach: U.S. Study of Executives & Managers," Sponsored by Experian® Data Breach Resolution, Kasım 2011, http://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf

[5] Ponemon Institute: "2012 Cost of Cyber Crime Study: United States," Ekim 2012. http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_ Study_FINAL6%20.pdf

İnsansız Hava Araçları ve Siber Güvenlik

BÖLÜM 15

Dr. Öğr. Üyesi İbrahim Alper DOĞRU
Dr. Murat DÖRTERLER
Emre UYAR

İNSANSIZ HAVA ARAÇLARI VE SİBER GÜVENLİK

Günümüzde insansız savaş uçakları, kamikaze ve sürü İHA gibi teknolojiler hızla gelişmekte ve yaygın olarak kullanılmaya başlamaktadır. Sağladığı fayda ve katkıların yanında karşılaşılabilecek tehdit ve tehlikelerde de artışlar beklenmektedir. Bu bölümde İHA sistemleri ve bu sistemlerde oluşabilecek siber güvenlik tehditlerine karşı alınabilecek önlemler sunulmuştur.

15.1. Giriş

Son yıllarda teknolojinin yüksek ivmeyle gelişmesinin bir sonucu olarak İnsansız Hava Araçları (İHA) hayatımızın çeşitli bölümlerinde yaygın olarak kullanılmaktadır. Söz konusu araçlar enerji hatları, su yönetim ve ulaşım sistemleri gibi kritik altyapıları izlemenin yanında afet kurtarma, hassas tarım ve hobi amaçlarıyla da kullanılabilmektedir. Ayrıca düşük maliyetinden dolayı son zamanlarda askeri alanlardaki kullanımlarıyla adından oldukça söz ettirmektedir.

Günümüzde dünya çapındaki çevrimiçi (online) satış siteleri, satın alınan ürünleri belirli bir ücret karşılığında İHA'lar ile alıcılarına ulaştırmaktadır. Yine ülke sınırlarından ilaç kaçakçılığı ve kritik lokasyonlardan görüntü alma gibi kullanım örnekleri çeşitli zamanlarda uluslararası medyanın gündemine oturmuştur. Fakat söz konusu araçlar daha çok askeri alandaki kullanım örnekleriyle ön plana çıkmaktadır.

Teknolojiden aktif olarak yararlanan devletler önceden insanların yürüttüğü faaliyetleri artık makinelere yaptırmaktadır. Bu makinelerin kullanımı kimi zaman ülkeler arasındaki ilişkilerde krizlere yol açabilmektedir. 2011 yılında İran tarafından Amerikan Hava Kuvvetleri'ne ait İHA'nın ele geçirilmesi, durumun ciddiyetini göz-

ler önüne sermektedir [1]. Silahlı İHA'ların da (SİHA) geliştirilmesiyle birlikte bilim kurgu filmlerinde yer alan robot savaşları sahnelerinin, yakın gelecekte gerçek olma ihtimali artmıştır.

Türkiye, savunma sanayii alanında son yıllarda büyük bir ivme ile önemli bir ilerleme kat etmiştir. Üretilen yerli ve milli araçlar ile bu alanda faaliyet gösteren diğer ülkelerle büyük bir rekabet içinde yer almaktadır. Türk Havacılık ve Uzay Sanayii A.Ş. (TUSAŞ) ve Baykar Makina gibi kuruluşlar tarafından üretilen İHA ve SİHA'lar savunma sanayimizin geldiği noktanın önemli bir göstergesidir [2]-[3]. Bunun bir sonucu olarak son yıllarda Türk Silahlı Kuvvetleri'nin (TSK) yurtiçi ve yurtdışında gerçekleştirdiği faaliyetlerde elde ettiği başarılarda İHA ve SİHA'ların önemli katkıları olmuştur.

Yapay zekâ uygulamaları ile birlikte sivil ve askeri amaçlar için üretilmiş mevcut İHA'ların yanında kamikaze ve sürü İHA'lar gibi teknolojiler de ilgi odağı olmaktadır. Tüm yaşanan gelişmeler göz önüne alındığında, İHA sistemlerinin yapısı gereği kablosuz haberleşme teknolojilerine bağımlı olması ve dronların interneti (The Internet of Drones) [4] kavramının da literatüre girmesiyle birlikte İHA'larda siber güvenlik kavramı büyük önem taşımaktadır.

15.2. İnsansız Hava Araçları Sınıfları

İHA'lar sahip oldukları özelliklere göre çeşitli sınıflara ayrılmaktadır. Oyun ve hobi amaçlı olarak model uçaklar kullanılırken; daha gelişmiş, uçuş bilgisayarına sahip olan ve önceden programlanabilen araçlar; izleme, takip, trafik yoğunluk kontrolü, afet kurtarma vb. amaçlarla kullanılabilmektedir. İHA'nın içerisinde bulunduğu radar, baz istasyonu, yer istasyonu ve komuta merkezi gibi bileşenlerin yer aldığı sistemler ise askeri amaçlarla kullanılmaktadır.

Avrupa'da askeri İHA üreticilerinin oluşturduğu "Avrupa İnsansız Araç Sistemleri Birliği" (The European Association of Unmanned Vehicle Systems-EUROUVS) tarafından 2006 yılında yapılan çalışmada İHA'lar; maksimum kalkış ağırlığı (kg), maksimum uçuş yüksekliği (m), havada kalma süresi (saat) ve veri haberleşme menzili (km) gibi özelliklere göre sınıflandırılmaktadır [2]. Tablo 15.1'de EUROUVS İHA sınıflandırması sunulmaktadır.

Tablo 15.1. EUROUVS İHA Sınıflandırması [2]

Kategori		Maksimum Kalkış Ağırlığı (kg)	Maksimum Uçuş Yüksekliği (m)	Havada Kalma/ Dayanım Süresi (saat)	Veri Haberleşme Menzili (km)
Mikro/Mini İHA	Mikro	0.1	250	1	<10
	Mini	<30	150-300	<2	<10
Taktik İHA	Yakın Menzil	150	3000	2-4	10-30
	Kısa Menzil	200	3000	3-6	30-70
	Orta Menzil	150-500	3000-5000	6-10	70-200
	Uzun Menzil	-	5000	6-13	200-500
	Dayanımlı	500-1500	5000-8000	12-24	>500
	Orta İrtifa Uzun Havada Kalış (MALE)	1000-1500	5000-8000	24-48	>500
Stratejik İHA	Yüksek İrtifa Uzun Havada Kalış (HALE)	2500-12500	15000-20000	24-48	>2000
Özel Görev İHA	Öldürücü	250	3000-4000	3-4	300
	Tuzak	250	50-5000	<4	0-500
	Stratosferik	-	20000-30000	>48	>2000
	Ekzosferik	-	>30000	-	-

Mikro/Mini İHA'lar genellikle teknoloji marketlerde satılan ve genellikle video çekimleri gibi sosyal amaçlarla kullanılan hava araçlarıdır. Taktik, stratejik ve özel görev İHA'lar ise genellikle askeri amaçlarla kullanılmaktadır. Ayrıca özel görev İHA'lar uzay araştırmalarında tercih edilmektedir.

2010-2011 yıllarında NATO tarafından yapılan sınıflandırmaya göre İngiltere Savunma Bakanlığı tarafından oluşturulan "Müşterek Doktrin 2/11" dokümanında sivil kategorinin eklenmesiyle birlikte İHA sistemleri 3 farklı sınıf altında incelenmiştir [5],[12]-[13]. Tablo 15.2'de NATO İHA sistemleri sınıflandırması sunulmaktadır.

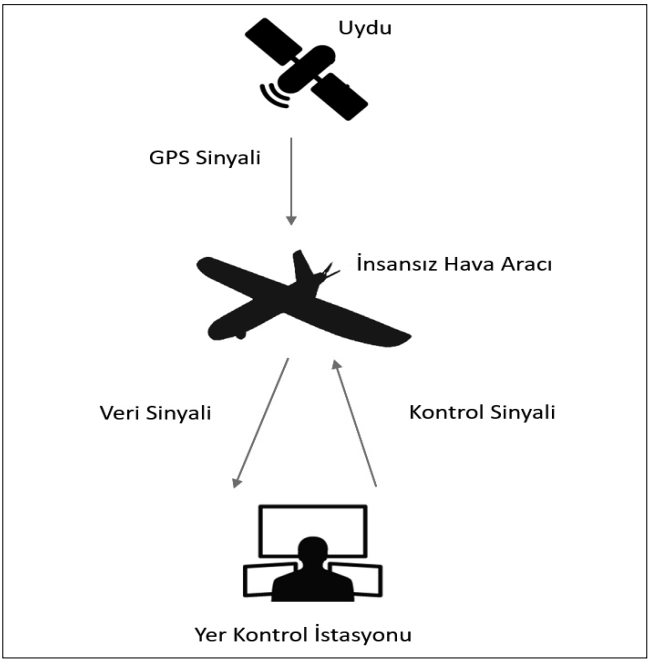
Tablo 15.2. NATO İHA Sistemleri Sınıflandırması [5]

Sınıfı	Kategorisi	Görev Yüksekliği (ft)	Görev Yarıçapı (km)	Sivil Kategori	Örnek Platform
Sınıf I (150 kg dan hafif)	Mikro (<2 kg)	<200 (AGL)	5 (LOS)	Ağırlık Sınıfı Grup 1 Küçük İHA (<20 kg)	Black Widow
	Mini (2-20 kg)	<3.000 (AGL)	25 (LOS)		Bayraktar, Malazgirt, Scan Eagle
	Küçük (> 20 kg)	<5.000 (AGL)	50 (LOS)	Ağırlık Sınıfı Grup 2 Hafif İHA (200-150 kg)	Hermes 90
Sınıf II (150-600 kg)	Taktik	<10.000 (AGL)	200 (LOS)	Ağırlık Sınıfı Grup 3 İHA (>150 kg)	Bayraktar Taktik, Karayel, Aerostar
Sınıf III (600 kg dan ağır)	Orta İrtifa Uzun Havada Kalış (MALE)	<45.000 (MSL)	Limitsiz (BLOS)		ANKA, Heron, Predator, Reaper
	Yüksek İrtifa Uzun Havada Kalış (HALE)	<65.000	Limitsiz (BLOS)		Global Hawk
	Saldırı/ Muharebe	<65.000	Limitsiz (BLOS)		X-47B, Phantom Ray
AGL: Zemin Seviyesi (Above Ground Level) LOS: Görüş Hattı (Line-of-Sight)					
MSL: Ortalama Deniz Seviyesi (Mean Sea Level) BLOS: Görüş Hattı Ötesi (Beyond-Line-of-Sight)					

Yukarıda belirtilen iki tablo arasındaki farklardan da anlaşılacağı üzere teknolojik gelişmeler doğrultusunda yeni geliştirilen hava araçlarının Tablo 15.1 ve Tablo 15.2'de belirtilen aralıkların dışına çıkabileceği göz önünde bulundurulmalıdır. Örneğin, yeni nesil piller ile mini bir İHA'nın Tablo 15.1'de belirtilen havada kalma süresi 2 saatin üzerine çıkabilmekte veya taktik bir İHA 8000 metrenin üzerinde uçabilmektedir. Sonuç olarak sınıflandırma açısından İHA'lar çok dinamik bir yapıya sahiptir.

15.3. İnsansız Hava Aracı Sistemleri

İnsansız hava aracı sistemleri; İHA, yer kontrol istasyonu ve İHA haberleşme ağından oluşmaktadır [14]. Şekil 15.1'de örnek bir İHA sistemi sunulmaktadır.



Şekil 15.1. İnsansız Hava Aracı Sistemi Örneği

15.3.1. İnsansız Hava Aracı Bileşenleri

İnsansız hava araçları genellikle 4 ayrı fakat bağımlı sistemlerin birleşiminden oluşmaktadır:

- **Veri Edinme Modülü:** İHA ortamından veri toplamaktan sorumlu sistemdir. Genellikle İHA üzerindeki sensörlerden elde edilen çevresel verileri kapsamaktadır.
- **Navigasyon Sistemi:** İHA'nın yönlendirilmesine ve yönetimine yardımcı olan sistemdir.
- **Kontrol Modülü:** İHA'yı bir operatör aracılığıyla manuel olarak ya da bir program aracılığıyla bağımsız olarak yönlendirmek için navigasyon sistemindeki verileri kullanan modüldür.
- **Veri Kayıt Modülü:** Verileri yer kontrol istasyonuna göndermeden önce geçici olarak kaydetmek için kullanılmaktadır.

15.3.2. Yer Kontrol İstasyonu Bileşenleri

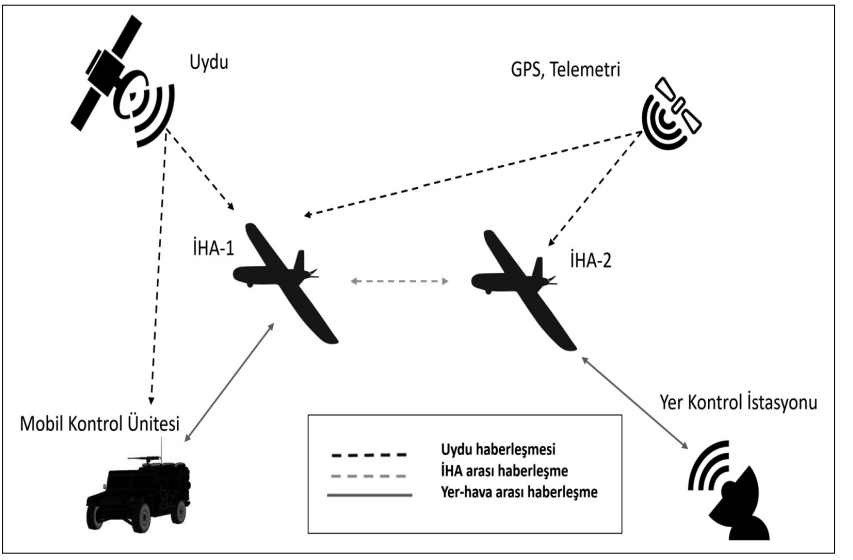
- **Operatör:** Operasyonlar sırasında İHA'ları kontrol etmek ve/veya izlemek için kullanılan bir kişi veya program olabilmektedir.

- **Veri Depolama Modülü:** İnceleme veya analiz için kullanılabilecek verilerin saklandığı kısımdır.
- **Veri Analiz Modülü:** İHA'dan alınan verilerden ve analitik için veri depolama modülünü kullanan iş istasyonlarından oluşmaktadır.

15.3.3. İHA Haberleşme Ağları

İHA'lar ve yer kontrol istasyonları arasında 2 farklı iletişim kanalı bulunmaktadır. İlki sinyal iletişim kanalıdır. Sinyal iletişimi genellikle yer kontrol istasyonundan İHA'ya gönderilmekte ve İHA'nın hareketlerini kontrol etmek için kullanılmaktadır. Diğeri ise veri iletişim kanalıdır. Gönderilen veriler çoğunlukla İHA'nın kontrolüne yardımcı olan sensör verilerinden ve izleme/görev yardımı amacıyla toplanan telemetri verilerinden oluşmaktadır.

İHA sisteminde iletişimin ağırlığı kablosuz teknolojiler üzerinden gerçekleştirilmektedir. Şekil 15.2'de İHA haberleşme ağları sunulmaktadır.



Şekil 15.2. İnsansız Hava Aracı Haberleşme Ağları

Veriler aşamalar halinde iletilmektedir. Sensörler önce verileri toplayarak İHA'ya iletmektedir. En yaygın veri iletişim yöntemleri aşağıdaki gibidir:

- **Kablolu Haberleşme:** Fiziksel bağlantıdır ve kısa sabit bağlantılar için daha etkilidir. Bu yöntem sensörleri İHA'ya bağlamak için kullanılmaktadır.
- **Kablosuz Haberleşme:** Bu iletişim şekli genellikle verileri iletmek için kullanılmaktadır. İHA'lar ve yer kontrol istasyonları arasında farklı kablosuz iletişim teknolojileri yer almaktadır.

Örneğin; Bluetooth, Zigbee ve Wi-Fi teknolojileri kısa mesafeler için tercih edilirken WiMAX ve hücresel şebekeler uzun mesafeler için kullanılmaktadır. Uydu iletişimi çoğunlukla GPS koordinatlarını İHA'lara, WiMAX ve hücresel şebekelerin bulunmadığı alanlarda iletmek için kullanılmaktadır.

15.4. İnsansız Hava Araçları Haberleşme Yöntemleri

İnsansız hava araçlarını kontrol etmek için çeşitli kablosuz haberleşme teknolojileri kullanılmaktadır. Kullanılan haberleşme teknolojisi, araçların kullanım amaçlarına göre değişiklik göstermektedir. Genellikle kullanılan teknolojiler aşağıdaki gibidir:

- Bluetooth
- Wi-Fi
- 3G/4G/LTE
- Uydu (Satellite)
- GPS
- Diğer Radyo Frekansları (2.4Ghz, 5.8Ghz, vb.)

Bluetooth teknolojisi kullanan araçlar sınırlı uçuş süresi ve 20 metre civarında kısa bir menzile sahiptir. Genellikle oyuncak serisi İHA'lar olarak sınıflandırılmaktadır. Wi-Fi teknolojisini kullanan araçlar da bluetooth teknolojisi gibi sınırlı uçuş süresi ve 50 metre civarında kısa bir menzile sahiptir. Yine aynı şekilde Wi-Fi haberleşmesi kullanan araçlar oyuncak ve hobi amaçlı olarak kullanılmaktadır.

Diğer radyo frekanslarını kullanan araçlar genellikle 900MHz, 1.3GHz ve 5.8GHz frekanslarında çalışmaktadır. Mikro/mini kategorilerine giren İHA'ların çoğunluğunda 2.4GHz ve 5.8GHz frekansları kullanılmaktadır. Bir frekans aracın kontrolünü sağlamaktayken diğeri ise video akışı için kullanılmaktadır. Genel olarak

mikro/mini İHA'lar yaklaşık 2 kilometre menzile sahipken doğru anten, alıcılar ve yeterli güç kapasitesi ile bu mesafe 75 kilometreye kadar çıkabilmektedir.

3G/4G/LTE teknolojisi, genellikle internet altyapısını kullanan uzun menzilli bir iletişim modelidir. Maksimum menzil, İHA'ların dayanıklılığı ve uygun mobil taşıyıcı sinyallerin tespit edilmesine bağlı olarak değişmektedir.

Uydu haberleşmesi, yüksek menzil gerektiren araçlarda ve genellikle askeri amaçlı olarak kullanılmaktadır. Otonom kontrol sağlamak amacıyla uydu teknolojileri ilave olarak Küresel Uydu Seyrüsefer Sistemlerinden (KUSS) faydalanılmaktadır. Askeri keşif, gözetleme, takip ve saldırı görevlerinde kullanılan İHA'lar bu teknolojilerden aktif olarak yararlanmaktadır.

KUSS teknolojisinin ilk örneği Amerika Birleşik Devletleri (ABD) Savunma Bakanlığı tarafından geliştirilen ve uzaya gönderilen 24 adet uydudan oluşan GPS (Global Positioning System; Küresel Konumlama Sistemi) sistemidir. İlk olarak yalnızca askeri kullanımlara açık olan bu sistem, 1980 yılından itibaren sivil kullanıma da açılmıştır. Günümüzde ise konum, hız, zaman gibi bilgilere ihtiyaç duyulan gerek endüstriyel gerekse de eğlence amaçlı birçok uygulamada kullanılır duruma gelmiştir [9]-[10].

GPS sisteminin dışında Rusya tarafından geliştirilen GLONASS, Avrupa Birliği tarafından geliştirilen Galileo, Çin tarafından geliştirilen Compass ve Hindistan tarafından geliştirilen IRNSS konumlandırma sistemleri mevcuttur. Ancak GPS dışındaki sistemlerin henüz yeterli olgunluk seviyelerine ulaşamadıkları için dünya genelinde GPS, ağırlıklı olarak neredeyse her alanda kullanılmaktadır [11].

Teknolojinin hızla gelişmesinin bir sonucu olarak yaygın kullanıma sahip olan GPS sistemi maalesef sivil alanda askeri alanda olduğu gibi yeterince güvenli değildir. Askeri uygulamalarda GPS verileri şifreli olarak iletilirken, sivil uygulamalarda veriler açık olarak iletilmektedir. Ayrıca söz konusu sistem, bozulmalara karşı çok hassastır.

15.5. İnsansız Hava Araçlarına Yönelik Müdahale Yöntemleri

Bütün teknoloji ürünlerinde olduğu gibi, İHA'lar da faydalı ya da kötü amaçlar için kullanılabilmektedir. İHA'lar kişisel mahremiyet ihlalinden, ulusal güvenlik ihlaline kadar geniş bir yelpazede yeni imkanlar sağlamaktadır. İHA'ların varlık göstermesiyle, özel hayatın gizliliği ve bireysel hak ve özgürlüklerin korunmasına yönelik geleneksel tedbirler yetersiz kalmıştır. Sosyal hayatın yanı sıra askeri ve casusluk amaçlarıyla kullanılan İHA'lar da başka ülkelere ait bilgilere keşif, gözetleme ve takip gibi faaliyetlerle ulaşarak devletlerarası krizlere yol açabilmektedir.

Kötü amaçlı kullanılan İHA'lara karşı müdahale yöntemleri geliştirilmiş ve geliştirilmeye devam etmektedir. Bunlar [6]:

- Pasif Önlemler
- Aktif Önlemler

Pasif önlemler, İHA'ların etki alanını kısıtlamaya yönelik dolaylı önlemlerdir. Kapıları otomatik kilitleme, görüntü kaydedilmesini engellemek için perdeleri kapatma, insanları uyararak güvenli alanlara yönlendirme gibi durumlar pasif önlemlere örnek verilebilmektedir.

Aktif önlemler ise doğrudan doğruya bir İHA'nın işlevini kısmen ya da tamamen kısıtlamaya yönelik girişimleri içermektedir. Bu yöntemler şu şekildedir:

- Müdahale İnsansız Hava Araçları
- Sinyal Engelleyici (Jammer)
- Ateşli Silahlar
- Elektromanyetik/Mikrodalga Işınlar
- Özel Yetiştirilmiş Yırtıcı Kuşlar
- Hekleme (hacking)

Şekil 15.3'te İHA'lara yönelik müdahale yöntemlerine ait görseller bulunmaktadır. Küçük İHA'ların etkisiz hale getirilmesi için kullanılan yöntemlerden biriside yırtıcı kuşlara dayanmaktadır. Bu kuş-

lar eğitilerek doğal avlarına yaptıkları saldırıya benzer bir şekilde İHA'ları da avlayabilmektedir (Bakınız Şekil 15.3a). Söz konusu yöntem kısa vadede başarılı gibi görünse de silahlı hava araçlarıyla hayvanlar engellenebilmektedir.

Müdahale hava araçları, hedef İHA'yı etkisiz hale getirmek amacıyla yakın mesafeden ağ atmaktadır (Bakınız Şekil 15.3b). Çok yetenekli pilot bulundurma, düşme riski ve yüksek maliyetli, güçlü araç bulundurma ihtiyaçları gibi dezavantajları bulunmaktadır.

Şekil 15.3. İnsansız Hava Araçlarına Yönelik Müdahale Yöntemleri

İHA'lar bünyelerindeki siber güvenlik zafiyetleri üzerinden de hedef alınabilmektedir (Bakınız Şekil 15.3c). Diğer adıyla heklemenin, diğer müdahale yöntemlerine göre maliyetsiz olması sebebiyle gelecekte en çok tercih edilecek yöntemler arasında olacağı öngörülmektedir.

Ateşli silahlar, İHA'ların özelliklerine göre düşük etki alanına sahiptirler (Bakınız Şekil 15.3d). Günümüzde İHA'ların ucuz maliyete sahip olması ve araçlar arasında etkileşimli ağların kurulması gibi özellikler göz önüne alındığında ateşli silahlar etkin bir seçim olarak görülmemektedir.

Elektromanyetik/Mikrodalga ışınları ateşli silahlarda olduğu gibi düşük etki alanına sahiptir (Bakınız Şekil 3e). Radarlar tarafından

tespit edilen İHA'ların kamera gibi elektronik donanımlarını bozmak için kullanılmaktadır. Ayrıca bu ışınları kullanmak, özel izin gerektirebilmektedir.

Hedef İHA'lar, Sinyal Engelleyici (Jammer) kullanılarak GPS ve radyo bağlantısı kesilerek etkisizleştirilebilmektedir (Bakınız Şekil 15.3f). Engellenen araç, sahip olduğu özelliğe göre düşme veya başlangıç koordinatlarına geri dönme gibi eylemler gerçekleştirmektedir. Düşman aracın faaliyetlerini engelleme ve düşman operatörün tespiti gibi avantajları bulunmaktadır. Diğer taraftan, bölgedeki diğer Wi-Fi, GPS, vb. kablosuz yayınları etkileme, otomatik pilotla uçan araçlarda etkili olamama ve yerleşim yerlerine düşme gibi riskleri barındırmaktadır.

15.6. İnsansız Hava Araçlarında Siber Güvenlik

İHA sistemleri yapısı gereği kablosuz haberleşme teknolojilerini aktif olarak kullanmaktadır. Öte yandan İHA, yer kontrol istasyonu ve sensörler gibi bileşenleri de bünyesinde barındırmaktadır. Her bir bileşen/teknoloji birtakım tehdit ve saldırılara maruz kalabilmektedir. Tablo 15.3'te İHA sistemlerine yönelik çeşitli tehdit/saldırı çeşitleri sunulmaktadır.

Uydu haberleşmesi uzun mesafelerde kullanılacak İHA'lar için vazgeçilmez bir teknolojidir. Ayrıca küresel konumlandırma sistemleri de uydu haberleşme teknolojisini kullanmaktadır. Söz konusu teknolojiler; zayıf şifreleme, trafik sebebiyle yaşanan yoğunluk ve sinyal kesme, hizmet engelleme gibi erişilebilirliğe yönelik saldırılarla istismar edilebilmektedir.

Öte yandan İHA'lar GPS aldatmacası ile farklı lokasyonlara yönlendirilmekte, yer kontrol istasyonunda bulunan sistemleri zararlı yazılım enjekte edilerek kullanılamaz hale getirilmekte, sensörler üzerindeki veriler manipüle edilebilmektedir. Ayrıca zararlı yazılımlar ile sistemlere ait gizli bilgiler çıkartılabilmektedir.

Tablo 15.3. İHA Sistemlerine Yönelik Başlıca Siber Tehditler [7]

Bileşen/Teknoloji	Tehdit/Saldırı
Uydu Haberleşmesi	Zayıf Şifreleme
	Trafik Sebebiyle Yaşanan Yoğunluk
	Erişilebilirliğe Yönelik Saldırılar(Sinyal Kesme, Hizmet Engelleme, vs.)
Diğer Radyo Haberleşme Bağlantıları	Gizliliği İfşa Edilmiş İHA'lar
	Gizli Dinleme
	Radyo Sinyali Kesme (Jamming) ve Hizmet Engelleme (DoS)
	Konum Gizliliği Saldırısı
İnsansız Hava Aracı	GPS Aldatmacası
	Fuzzing Saldırısı
	Ele Geçirme ve Etkisiz Hale Getirme
	Kazanç Ayarlama Saldırısı
Yer Kontrol İstasyonu	Zararlı Yazılım Enjeksiyonu
	Keylogger ve Diğer Veri Çıkarma Mekanizmaları
	Zayıf Kimlik Doğrulama
Komuta ve Kontrol Mesajları	Zayıf Mesaj Doğrulaması
	Kontrol Kanalı Sinyal Engelleme
Sensör/Algılayıcı	Sensör ve Çalıştırıcı Manipülasyonu
	Aldatmaca

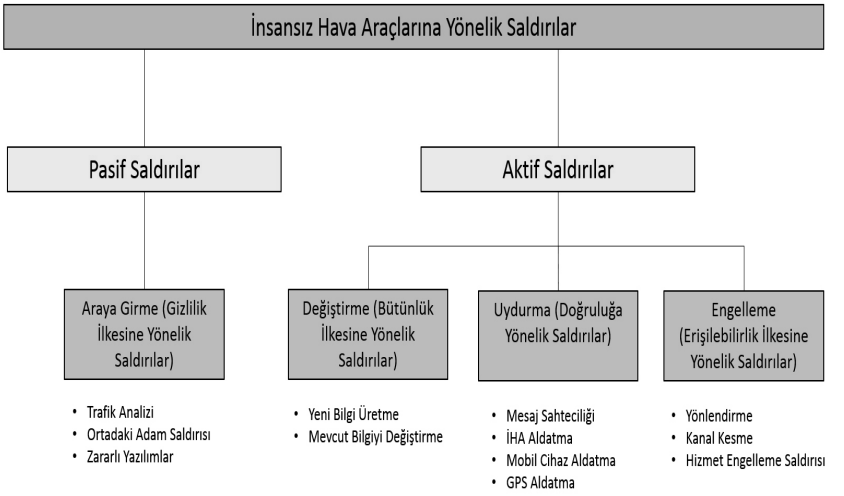
Özetle, yukarıda belirtilen bileşen/teknolojiler siber güvenliğin gizlilik, bütünlük ve erişilebilirlik ilkelerine zarar verebilecek çeşitli tehdit ve saldırılara maruz kalabilmektedir.

Deprem, sel gibi doğal afetler veya sabotaj eylemleri sonucunda temel iletişim kanallarının kesildiği acil durumlarda İHA destekli ağlar ile oluşabilecek mağduriyetler giderilebilmektedir. İHA'lar mobil istasyon, yönlendirme noktası ve uç terminal olarak kullanılabilmektedir. Böylelikle İHA'lar bir baz istasyonu görevi alarak iletişim altyapısı oluşturmaktadır.

Bu gibi kritik kullanım amaçları göz önünde bulundurulduğunda İHA sistemlerinde bulunan donanım, yazılım ve haberleşme protokollerinde yer alan güvenlik zafiyetleri ve tehditler risk oluşturmak-

tadır. İHA'lara pasif ve aktif olmak üzere çeşitli saldırılar gerçekleştirilebilmektedir.

Siber güvenliğin gizlilik ilkesine yönelik; trafik analizi, ortadaki adam saldırıları gibi pasif saldırılar yapılabilirken, bütünlük ilkesine yönelik yeni bilgi üretme ve mevcut bilgiyi değiştirme, erişilebilirlik ilkesine yönelik; yönlendirme, kanal kesme ve hizmet engelleme ile son olarak doğruluğa yönelik; mesaj sahteciliği ve aldatmaca saldırıları gibi aktif saldırılar yapılabilmektedir. Şekil 15.4'te İHA sistemlerine yönelik saldırılar sunulmaktadır.



Şekil 15.4. İHA Sistemlerine Yönelik Yapılan Siber Saldırılar [8]

Genel güvenlik tehditleri ve alınması gereken önlemler Tablo 15.4'te sunulmaktadır. Siber güvenliğin gizlilik, bütünlük ve erişilebilirlik ilkeleri çeşitli saldırı yöntemleriyle zarara uğratılmaya çalışılmaktadır.

Saldırganlar, Tablo 15.4'te belirtilen yöntemlerle İHA sistemlerine tehdit oluşturmaktadır. Hekleme, gizlice dinleme, kimlik aldatmacası ve ağ saldırılarında verilerin açık metin olarak iletildiği durumlara saldırganlar kolaylıkla verilere erişebilmektedir. Bu gibi durumlar için veriler şifrelenmelidir.

Verilerin iletilmesi ve depolanması sırasında saldırganlar tarafından araya girme saldırılarıyla veriler değiştirilebilmektedir. Mesaj doğrulama kodu gibi özet (hash) fonksiyonları ile veri bütünlüğünün sağlanması için önlem alınabilmektedir.

Tablo 15.4. Genel Güvenlik Tehditleri ve Alınması Gereken Önlemler [8]

	Tehdit	Kategori	Önlem
1	Saldırganlar; hekleme, gizlice dinleme, kimlik aldatmacası ve katmanlar arası ağ saldırıları yoluyla bağlantıların güvenliğini tehlikeye atabilmektedir.	Gizlilik İlkesine Yönelik Saldırılar	Verilerin şifrelenmesi
2	Saldırganlar verilerin iletilmesi ve depolanması sırasında verileri değiştirebilmektedir.	Bütünlük İlkesine Yönelik Saldırılar	Mesaj doğrulama kodu gibi özet (hash) fonksiyonları
3	Saldırganlar haberleşme kanallarını engelleyebilmekte ve ağlara yönelik hizmet engelleme saldırıları gerçekleştirebilmektedir.	Erişilebilirlik İlkesine Yönelik Saldırılar	Güçlü kimlik doğrulama ile olay tespit ve raporlama mekanizmaları
4	Saldırganlar İHA sisteminde depolanan verilere yetkisiz erişim sağlayabilmekte ve verileri değiştirme yetkisi kazanabilmektedir.	Doğruluk İlkesine Yönelik Saldırılar	Verilere erişimde kimlik doğrulama ve şifreleme

Saldırganlar haberleşme kanallarını engelleyebilmekte ve ağlara yönelik hizmet engelleme saldırıları gerçekleştirebilmektedir. Güçlü kimlik doğrulama, olay izleme (monitoring) ve raporlama mekanizmaları ile belirtilen saldırılara karşı önlem alınabilmektedir.

İHA sistemlerinde depolanan verilere yetkisiz erişim sağlanabilmekte veriler yetkisiz kişiler tarafından değiştirilebilmektedir. Verilere erişimde kimlik doğrulama ve şifreleme mekanizmaları kullanılmadır.

Söz konusu tehditlere yönelik verilerin şifrelenmesi, mesaj doğrulama kodlarının kullanılması, olay tespit ve raporlama mekanizmaları ve verilere erişimde güçlü kimlik doğrulama gibi çeşitli tedbirlerin alınması gerekmektedir. Gerekli tedbirlerin alınması durumunda saldırganlar için caydırıcı bir duvar örülmüş olacaktır. Ayrıca Tablo 15.5'te İHA sistem güvenliğini tehdit eden detaylı saldırı yöntemleri belirtilmektedir.

15.7. Değerlendirmeler

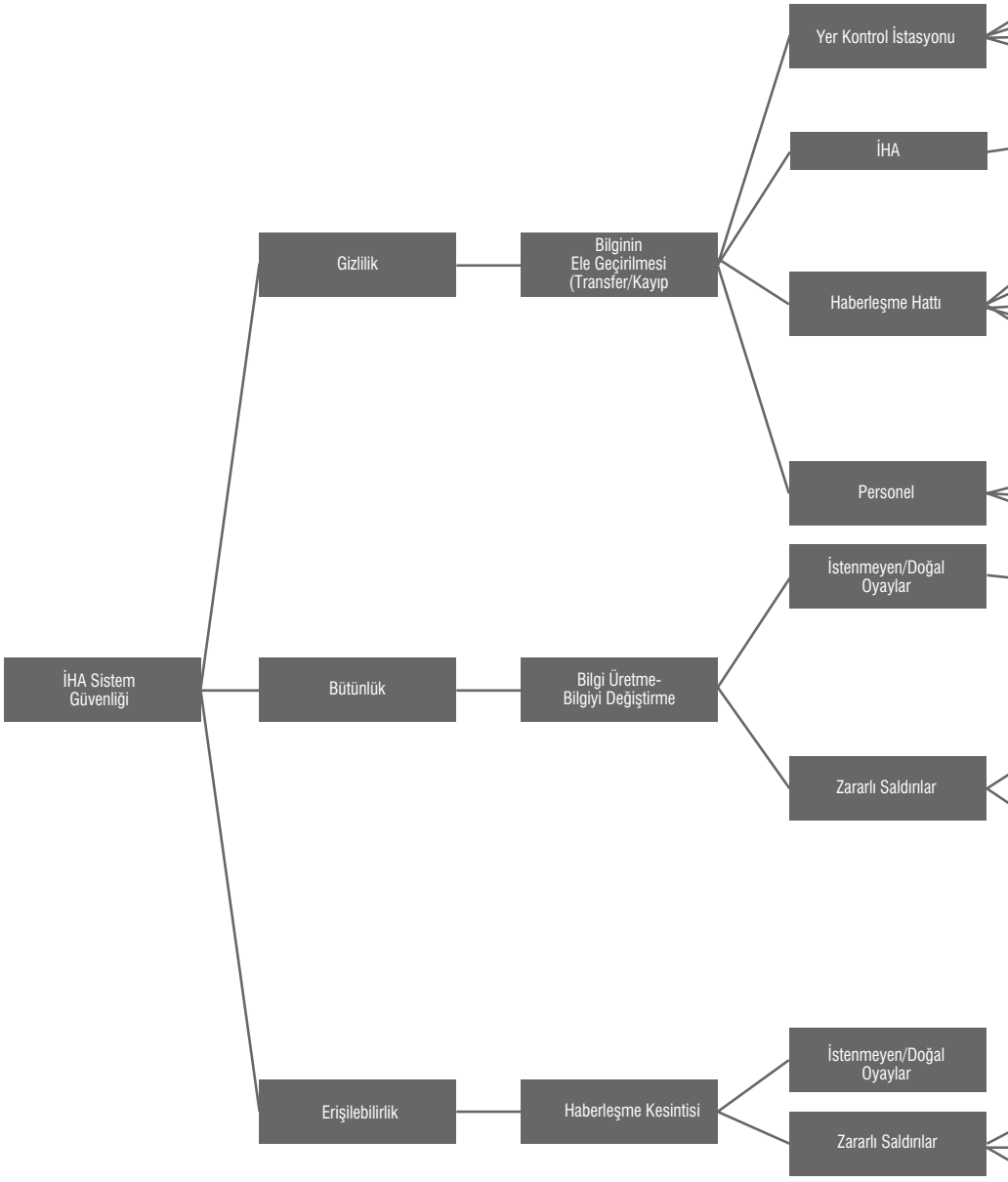
Tablo 15.5'ten de görülebileceği gibi teknoloji ile birlikte İHA sistemlerinin sürekli olarak gelişmesi, siber güvenlik açısından çeşitli zafiyetleri beraberinde getirmektedir. İHA teknolojisi hızlı bir şekilde gelişmiştir. Bu gelişim sayesinde kullanım alanları giderek yaygınlaşmaktadır.

Tüm gelişmelerin sonucunda İHA'larda siber güvenlik konusu büyük önem taşımaktadır. Bu alanda literatürdeki çalışmaların az bulunması, henüz çok bakir bir alan olduğunu göstermektedir. 2011 yılında Amerikan Hava Kuvvetleri'ne ait İHA'nın İran tarafından ele geçirilmesinin akabinde, İranlı mühendisler tarafından GPS aldatmacası yönteminin kullandığı bilgisinin iletilmesiyle literatüre GPS aldatmacası konusunda çeşitli çalışmalar girmiştir.

Yakın gelecekte insansız savaş uçakları, kamikaze ve sürü İHA'lar gibi teknolojilerin yapay zekâ uygulamaları ile birlikte gelişmesiyle birlikte İHA'larda siber güvenlik konusu giderek önem kazanacaktır.

İHA'lardaki her bir bileşen ve kullanılan her bir teknoloji bir saldırı alanı oluşturmaktadır. Bu alanlara yönelik gerçekleştirilebilecek tüm tehdit ve saldırılar derinlemesine araştırma gerektirmektedir.

Ülkemizde üretilen yerli ve milli İHA'lara yönelik gerçekleştirebilecek saldırılar göz önüne alındığında, bu araçların siber güvenlik açısından test edilmesi bir gereklilik olarak değerlendirilmelidir.



Tablo 15.5. İHA Sistem Güvenliğini Tehdit Eden Saldırılar [15]


Virüs
Zararlı Yazılım
Klavye Kaydedici
Truva Atı
Hekleme
Kimlik Aldatması
Çapraz Katman Saldırısı
Veri Çalma
Protokol Tabanlı Saldırılar
Çoklu Protokol Saldırısı
Dinleme
Sosyal Mühendislik
Personel Zafiyeti
İstenmeyen Aksiyonlar
Sinyal Bütünlüğü
Bozulmuş Bağlantı
Zararlı Kod
Altyordam İstismarı
Kablosuz Tehditler
Paket Yakalam Değiştirme ve Yeniden İletme
Sinyal Bütünlüğü
Bozulma
Artan SNR
Engelleme ve Yeniden İletme
Engelleme
Dos/DDos
Sahte Kontrol Sinyali/Komutları Üretme
Bellek Aşımı
Paket Yollama
Aldatma
UDP
SYN
ICMP
Ping

Kaynaklar

[1] Rodday N., "Exploring Security Vulnerabilities of Unmanned Aerial Vehicles, University Of Twente", July 2015, Amsterdam.

[2] Türk Havacılık ve Uzay Sanayii A.Ş., Url: www.tai.com.tr.

[3] Baykar Makina, Url: baykarmakina.com.

[4] Gharibi, M., Boutaba R., Waslander S. L., "Internet of Drones", University of Waterloo, 2016.

[5] Karaağaç C., "İHA Sistemleri Yol Haritası, Geleceğin Hava Kuvvetleri 2016-2050", STM.

[6] Lamprect J., "The Pros and Cons of Active and Passive Drone Countermeasures", Url: www.informationsecuritybuzz.com, April 2016.

[7] Javaid A. Y., "Cyber security threat analysis and attack simulation for unmanned aerial vehicle network, University of Toledo", 2015.

[8] He D., Chan S., Guizani M., "Drone-Assisted Public Safety Networks: The Security Aspect, IEEE Communications Magazine", August 2017.

[9] Haider Z., Khalid S., "Survey on Effective GPS Spoofing Countermeasures", Bahria University, IEEE, 2016.

[10] Gps.gov, Official U.S. "Government Information About The Global Positioning System (GPS) and Related Topics", 2018. url: http://www.gps.gov/ (06.02.2018).

[11] Bernal S. A. S., "Detection Solution Analysis For Simplistic Spoofing Attacks in Commercial Mini And Micro UAVs, University Of Tartu", Master's Thesis, 2016.

[12] United Kingdom DoD, "Joint Doctrine 2/11 The UK Approach to Unmanned Aircraft Systems", 30 March 2011.

[13] NATO Joint Air Power Competence Center (JAPPC), "Strategic Concept of Employment for Unmanned Aircraft Systems in NATO", 04 Ocak 2010.

[14] Benkraouda H., Barka E., Shuaib K., "Cyber-Attacks on The Data Communication of Drones Monitoring Critical Infrastructure", College of Information Technology, United Arab Emirates University, 2018.

[15] Javaid A. Y., Alam M., Sun W., Devabhaktuni V. K., "Cyber Security Threat Analysis and Modelling of an Unmanned Aerial Vehicle System", IEEE, 2012.

Yazarların Özgeçmişleri

Doç. Dr. Sedat AKLEYLEK

- Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü, Samsun.

Doçent Doktor, Samsun Hesaplamalı Bilimler Doktora Programı A.B.D. Başkanı.

Doç. Dr. Sedat Akleylek, İzmir doğumludur. 2004 yılında Ege Üniversitesi Matematik Bölümü'nde lisans eğitimini tamamlamıştır. Öğretim Üyesi Yetiştirme Programı kapsamında sırasıyla 2008 ve 2010 yıllarında yüksek lisans ve doktora çalışmalarını ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Programı'nda tamamlamıştır. 2012 yılında Almanya Bochum Ruhr Üniversitesi Donanım Güvenliği Grubu'nda, Almanya'da ve 2014-2015 yıllarında Almanya Darmstadt Teknik Üniversitesi Kriptografi ve Bilgisayar Cebri Grubu'nda misafir öğretim üyesi olarak görev almıştır. 2016 yılında Bilgisayar/Bilişim Bilimleri ve Mühendisliği, Bilgi Güvenliği ve Kriptoloji alt alanında doçent ünvanını almıştır.

Doç. Dr. Sedat Akleylek, kuantum sonrası kriptografi, verimli kriptografik hesaplamalar, Boolean fonksiyonlar ve siber güvenlik için uygulamalı kriptografi alanlarında çalışmalarını sürdürmektedir. Ulusal ve uluslararası kapsamda bilgi güvenliği ve kriptoloji alanında TÜBİTAK, KOSGEB, Üniversite-Sanayi İşbirliği Projeleri ve Üniversiteler tarafından desteklenen Bilimsel Araştırma Projelerinde yürütücü, araştırmacı ve danışman olarak görevler almıştır. Doç. Dr. Sedat Akleylek, uluslararası saygın iki dergide bilgi güvenliği ve kriptoloji alan editörlüğü görevlerini sürdürmektedir.

Murat AKIN

- Gazi Üniversitesi TUSAŞ Kazan Meslek Yüksek Okulunun Öğretim Görevlisi.

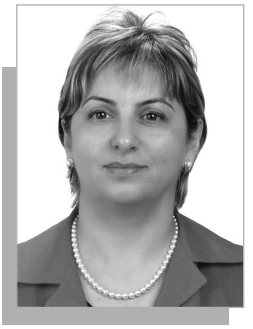
Lisans eğitimini Kocaeli Üniversitesi Bilgisayar Mühendisliğinde, yüksek lisansını Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği ABD tamamlamıştır. Doktora eğitimine Gazi Üniversitesinde devam etmektedir. İlgi alanları Siber Güvenlik, Büyük Veri ve Makine Öğrenmesidir.

Prof. Dr. Ramazan BAYINDIR

- Gazi Üniversitesi, Teknoloji Fakültesi Elektrik-Elektronik Mühendisliği Bölümü Öğretim Üyesi.

2015-2018 yıları arasında Bölüm Başkanlığı yapmıştır. Lisans düzeyinde Güç Sistemleri, Enerji İletimi ve Güç Sistemlerinde İzleme ve Koruma konularında, Lisansüstü düzeyinde de Modern Güç Sistemleri ve Şebeke Uygulamaları ile Dağıtık Üretim Sistemleri ve Şebeke Bağlantıları alanlarında dersler vermektedir. IEEE destekli ICRERA 2012-2018, POWERENG 2013, PEMC 2014 konferanslarında program yürütücüsü olarak görev yapmış, aynı zamanda SCI'da taranan ve uluslararası kabul görmüş önemli dergiler için misafir editörlük ve hakemlik gibi görevlerde bulunmuştur.

Halen Gazi Üniversitesi Fen Bilimleri Enstitüsü PARTC: Tasarım ve Teknoloji Dergisinin Editörü ve TÜBİTAK Turkish Journal of Electrical Engineering & Computer Sciences dergisinde Editörler Kurulu üyesidir. Yenilenebilir Enerji Teknolojileri, Akıllı Şebekeler ve Mikroşebekeler konularında uluslararası dergilerde ve konferanslarda 100'ün üzerinde makalesi ile bildirisi yayınlanmış olup, çalışmaları 800'ün üzerinde atıf almıştır. Farklı alanlardaki eğitim ve müfredat tasarımı ve geliştirilmesi, uluslararası düzeyde projelerin organizasyonu, planlanması ve yönetilmesi projelerinde görev almış olup, IEEE üyesidir.

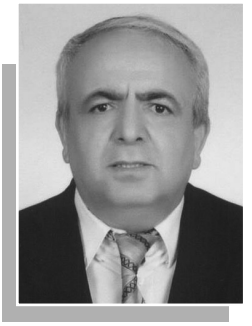


Prof. Dr. Türksel Kaya BENSGHIR

- Hacı Bayram Veli Üniversitesi

Prof. Dr. Türksel Kaya Bensghir Türkiye ve Orta Doğu Amme İdaresi Enstitüsünde Öğretim üyesidir. Haziran 2009- Temmuz 2016 arasında TODAİE eDevlet Merkezi (eDEM) Müdürü olarak çalışmıştır. Prof. Bensghir, 2013 yılından beri Birleşmiş Milletler Ekonomik Sosyal Konseyin bir organı olan CEPA- Kamu Yönetimi Uzmanlar Komite üyesi seçilmiş ve Komite çalışmalarına Türkiye temsilcisi olarak eDevlet alanında katkıda bulunmaktadır. Yönetim Bilişim Sistemleri alanında Prof. olan Kaya Bensghir, TODAİE,

Gazi Üniversitesi, Başkent üniversitesi olmak üzere üniversitelerde yönetim bilişim sistemleri, bilgi yönetimi, siber güvenlik ve yönetim, bilgi teorisi ve e-devlet olmak üzere, BT ve örgütsel değişim, sistem analizi, bilgi sistemleri tasarımı, e-iş ve e-ticaret konularında dersler ve kamu personeline e-devlet, bilgi yönetimi, e-imza, sistem dinamikleri, vb konularda seminerler vermektedir. Kaya Bensghir'in, Bilgi Teknolojileri ve Örgütsel Değişim başlıklı kitabı ve ortak yazarlı (F. Topcan) Türkiye'de E-imza: Kamu Kurumlarına Uygulanması, (A. Akay) Yerel Yönetimlerde Coğrafi Bilgi Sistemleri–Türkiye Uygulamaları kitabı ile yurt içi ve yurt dışında basılan editörlü kitaplarda yayınlanan çalışmaları bulunmaktadır. Ayrıca, yönetim bilişim sistemleri, e-imza, kamu görevlilerinin yetiştirilmesinde BT eğitimi, halkla İlişkiler ve web teknolojileri ve belediye web sitelerinin değerlendirilmesi, e-yerel yönetimler, belediyelerde CBS kullanımı, internet kafeler, kamu yöneticilerin ve vatandaşların e-devletten beklentileri vb konularda çeşitli araştırmaları, ulusal ve uluslararası toplantılarda sunulan bildirileri ve yurt içi ve yurt dışında yayınlanmış makaleleri vardır. Kaya Bensghir, TODAİE ve üniversitelerde bilişim konularında yüksek lisans ve doktora tez danışmanı ve tez kurul üyesi olarak görev almaktadır. Amme İdaresi Dergisi ve Çağdaş Yerel Yönetimler Dergisi -TODAİE; Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi (İİBF) Dergisi, Selçuk Üniversitesi Karaman İİBF Dergisi, Akdeniz Üniversitesi İİBF Dergisi ve Polis ve Sosyal Bilimsel Dergisi ve International Journal of Informatics Technologies (IJIT) dergisinde hakem kurul üyeliğinde bulunmaktadır. Kaya Bensghir 1996 dan beri Türkiye Bilişim Derneği üyesidir. Ayrıca Mobile Government Consortium International ve. European Conference on E-government ile yurt içinde gerçekleştirilen e-devlet ve bilişim konulu konferanslarda kurul üyeliğinde bulunmaktadır.



Prof. Dr. Yaşar BİLGE

1960 Sarıkamış doğumlu. Ankara Üniversitesi Tıp Fakültesinden 1985 yılında mezun oldu. Yalvaç Kapalı Cezaevi hekimliği yaptı. 1993 yılında Adli Tıp Uzmanı oldu. 2000 yılında doçent, 2008 yılında Profesör oldu. Adli Tıp Kurumu Ankara Grup Başkanlığı yaptı.

Ankara Üniversitesi Tıp Fakültesi Adli Tıp Anabilim Dalı öğretim üyesi. Tıp, Hukuk, Diş

Fakültelerinde adli tıp dersleri vermiştir. 100 den fazla akademik makalesi bulunan Prof Dr. Yaşar Bilge'nin ilgi alanları içerisinde Tıpta Uygulama Hataları alanında, eğitim ve öğretim, akreditasyon yer almaktadır. Evli ve iki çocuk sahibidir.

Gürol CANBEK

İstanbul Teknik Üniversitesi, Kontrol ve Bilgisayar Mühendisliği Bölümü'nden mezun oldu. Yüksek lisansını Gazi Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde yaptı. Orta Doğu Teknik Üniversitesi, Bilişim Sistemleri'nde doktora tezini çalışmaktadır. Bilgi güvenliği ve siber güvenlik üzerine çok sayıda akademik makalesi ve "Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri" (Grafiker Yayınları, 2006) başlıklı bir kitabı vardır.

Doç. Dr. Murat CENK

- ODTÜ Uygulamalı Matematik Enstitüsü Müdür Yardımcısı

Doktora derecesini ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi programından 2009 yılında almıştır. Daha sonra Eylül 2010'dan Ocak 2014 tarihine kadar, Kanada'daki Waterloo Üniversitesinin Elektrik ve Bilgisayar Mühendisliği bölümünde kriptografik algoritmaların verimli gerçekleştirilmesi üzerine doktora sonrası araştırmacı olarak çalışmıştır. 2014 yılından itibaren ODTÜ Uygulamalı Matematik Enstitüsünde öğretim üyesi olarak çalışmakta olan Murat Cenk'in araştırma konuları kriptografik algoritmaların verimli gerçeklenmesi, uygulamalı kriptografi ve kuantum sonrası kriptografidir.

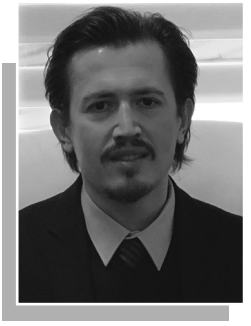
Dr. Murat DÖRTERLER

- Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Görevlisi, Ankara

Kayseri doğumlu olan Dörterler, 2005 yılında Gazi Üniversitesi Bilgisayar Sistemleri Anabilim Dalında Lisans eğitimini tamamladı. Aynı ünivresitenin Elektronik-Bilgisayar Anabilim Dalı'ndan 2008 yılında yüksek lisans, 2013 yılında doktora derecelerini aldı.

2005 yılında Milli Eğitim Bakanlığında çalışma hayatına başlayan Dörterler, 2009 yılına kadar bakanlığın taşra ve merkez teşkilatlarında eğitim-öğretim ve e-dönüşüm süreçlerinde görevler almıştır. 2009 yılından günümüze kadar Gazi üniversitesinin çeşitli birimlerinde akademik çalışmalarını sürdürmektedir.

Dörterler'in Yapay Zekâ, Zeki Optimizasyon, Gömülü Sistemler, Yazılım, Dağıtık Sistemler, Bilgi Güvenliği başta olmak üzere çeşitli alanlarda ulusal ve uluslararası mecralarda bildiri, yayın ve projeleri bulunmaktadır. Gazi Mühendislik Bilimleri Dergisi'nin editörlüğünü yapmaktadır. İyi derecede İngilizce bilmektedir. Evli ve İki çocuk babasıdır.



Dr. Öğretim Üyesi İbrahim Alper DOĞRU

- Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü, Öğretim Üyesi, Ankara

Tokat ili Erbaa ilçesinde doğan İbrahim Alper DOĞRU, İlk ve Orta Öğrenimini Tokat'ta tamamladı. Atılım Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliğinden Mezun olduktan sonra Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığında Bilgisayar Mühendisi olarak göreve başladı. Yüksek Lisansını Gazi Üniversitesinde Bilgisayar Mühendisliği Anabilim Dalında tamamladı. Doktorasını Gazi Üniversitesinde Elektronik Bilgisayar Eğitimi Anabilim Dalında tamamlamıştır.

2014-2017 Yıllarında Emniyet Genel Müdürlüğü Bilgi İşlem dairesi başkanlığında Bilgisayar Mühendisi olarak görev yaptı. 2017-2018 Yılların-

da Başbakanlık Gümrük Müsteşarlığı Elektronik ve Muhabere Dairesi Başkanlığı çözümleyici olarak görev yaptı. 2018-2011 Yıllarında Sosyal Güvenlik Kurumu Hizmet Sunumu Genel Müdürlüğünde bilişim uzmanı olarak görev yaptı. 2011-2013 Yıllarında Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliğinde Araştırma Görevlisi olarak görev yaptı. 2012 Yılında Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümüne Doktor Öğretim Üyesi olarak atandı aynı bölümde akademik çalışmalarını sürdürmektedir.

Araştırma alanları arasında Mobil Güvenlik, Nesnelerin İnterneti, Büyük Veri ve Sosyal Ağlar bulunmaktadır. Nesne Yönelimli Programlama, Mobil Programlama, Mobil Güvenlik, Nesnelerin İnterneti, Sosyal Ağ Analizi ve Güvenliği, Ağlarda Adli Bilişim gibi lisans ve lisansüstü dersleri vermektedir.

Dr. Ahmet EFE

- Ankara Kalkınma Ajansı İç Denetçisi, CISA, CRISC, PMP

Doğubayazıt doğumlu olan EFE, iktisat, kamu yönetimi, e-devlet ve siber güvenlik alanlarında çok disiplinli çalışmalar yapmaktadır. Kamu sektöründe müfettişlik, yöneticilik ve iç denetçilik kariyerinde çalışmaya devam etmekte olup, Certified Information Systems Auditor (CISA), Certified in Risk and Information Control (CRISC) ve Project Management Professional (PMP) gibi uluslararası kabul gören mesleki sertifikaları vardır. Yıldırım Beyazıt Üniversitesi Bilgisayar Mühendisliği Bölümünde siber güvenlik ile ilgili yüksek lisans ve doktora düzeyinde dersler vermektedir. Yayımlanmış 5 kitabı ve 46 Makalesi ile 2018 yılında ISACA tarafından BT Alanında en iyi yazar ödülüne layık görülmüştür. Evli 4 çocuklu olan Dr. Efe; İngilizce ve Arapça bilmektedir.

Dr. Mehmet Bedii KAYA

İstanbul Bilgi Üniversitesi Hukuk Fakültesi mezunudur. 2009 yılında İstanbul Bilgi Üniversitesi Ekonomi Hukuku yüksek lisans programını "Teknik ve Hukuku Boyutlarıyla İnternete Erişimin Engellenmesi" başlıklı teziyle tamamlamıştır. 2014 yılında Nottingham Üniversitesi'nde "Sürdürülebilir Kamu Alımlarının Regülasyonu" başlıklı teziyle hukuk doktorasını tamamlamıştır. Akademik kariyerine Nottingham Üniversitesi Hukuk Fakültesinde araştırma görevlisi olarak başlayan Dr. Mehmet Bedii KAYA, Ankara Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi'nde İdare Hukuku Ana Bilim Dalında öğretim üyesi olarak çalışmaktadır. Aynı zamanda, İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü'nde öğretim görevlisi sıfatıyla internet hukuku, e-devlet ve dijital demokrasi derslerini vermektedir. Dr. Mehmet Bedii Kaya, internet hukuku, elektronik haberleşme hukuku, adli bilişim ve siber güvenlik alanlarında çalışmalarını sürdürmektedir.

Prof. Dr. Şeref SAĞIROĞLU

- Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölüm Başkanı, Ankara

Prof. Sağıroğlu, ülkemizde bilgi güvenliği, siber güvenlik ve büyük veri bilimi, analitiği, güvenliği ve mahremiyeti konularında çalışmalar yapmaktadır. Bilgi Güvenliği, Siber Güvenlik, Yapay Zeka, Makine Öğrenme, Casus Yazılımlar ve Korunma Yöntemleri, Büyük Veri, Etkin Bilişim Teknolojileri Kullanımı, Ulusal Atıf İndeksi gibi konular ile uluslarası konferans bildiri kitabı editörlükleri olmak üzere 20'nin üzerinde yayınlanmış kitabı bulunmaktadır. Bu kitaplardan sonuncusu "Büyük Veri Analitiği, Güvenliği ve Mahremiyeti" olup ülkemizde bu alanda yayımlanan ilk akademik kitap olup, açık kaynak olarak okuyuculara sunulmaktadır. Biri amerikan patenti olmak üzere 4 patenti, 100'ün üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi ile 300'e yakın ulusal ve uluslararası yayımlanmış bildirisi ve 4.000'e yakın atıfı bulunmaktadır.

Uluslararası Bilgi Güvenliği Mühendisliği Dergisi (www.dergipark.gov.tr/ubgmd) ile International Journal of Information Security Science (www.ijiss.org) dergilerinin baş editörlük görevini yürütmektedir. Ayrıca aylık yayımlanan CyberMag Dergisinin de editörüdür.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (www.iscturkey.org), IEEE Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı (www. ubmk.org), IEEE Uluslararası Makine Öğrenmesi ve Uygulamaları Konferansı Büyük Veri ve Siber Güvenlik Oturumu (www.icmla-conferences.org/ icmla2017), Büyük Veri Analitiği, Güvenliği ve Mahremiyeti Ulusal Kamu Çalıştayı (bigdatacenter.gazi.edu.tr), Ulusal Siber Terör Konferansı (www.siberteror.org), Açık Veri Türkiye Konferansı (www.acikveriturkiye.org), Siber Güvenlik ve Savunma Çalıştayı (www.iscturkey.org) gibi konferansların başkanlığını veya eşbaşkanlığını yürütmektedir.

Bilgi Güvenliği Derneği (BGD), Türk Bilim Araştırma Vakfı (TÜBAV), Geleceği Önemseyenler Derneği (GÖNDER) Kurucu Üyesidir. İki dönem, BGD Yönetim Kurulu Başkanlığı ve TÜBAV Genel Başkanlığı Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürlüğü gibi görevleri yürütmüştür. BTK, Havelsan ve Kişisel Verileri Korumu Kurumuna danışmanlık yapmıştır.

Gönüllü olarak pek çok sosyal projeyi de yürütmüş olan Sağıroğlu, TÜBİTAK, Avrupa Birliği, BAP gibi Bilimsel Araştırma Projelerinde görev almıştır.

Ulusal ve uluslararası konferanslarda, Bilgi Güvenliği, Büyük Veri, Siber Güvenlik ve Savunma, Yapay Zeka, Biyometrik Uygulamalar, İnovasyon Kültürü Oluşturma gibi konularda davetli konuşmacı olarak seminer ve konferanslar vermektedir.

Halen; Gazi Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanlığı, FutureTech Genel Müdürü, BIDISEC Merkez Laboratuvarı Sorumlusu, Yüksek Öğretim Kurulu Siber Güvenlik Çalışma Grubu Üyeliği, Bilim Sanayi ve Teknoloji Bakanlığı Yazılım Sektörü Çalışma Grubu Üyeliği, Bilgi Güvenliği Derneği Yönetim Kurulu Üyeliği ve II. Başkanı gibi görevleri yürütmektedir.

Doç. Dr. Muharrem Tolga SAKALLI

- Trakya Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölüm Başkanı, Edirne

Lüleburgaz doğumludur. 1997 yılında İTÜ Kontrol ve Bilgisayar Mühendisliğinde Lisans eğitimini tamamlamıştır. 1999-2007 yılları arasında Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünde araştırma görevlisi olarak çalışmıştır. Yüksek lisans ve doktora çalışmalarını yine aynı üniversitede sırasıyla 2002 ve 2006 yıllarında tamamlamıştır. 2006 yılında KU Leuven Üniversitesi COSIC (Computer Security and Industrial Cryptography) araştırma gurubunda eStream projesi kapsamında 4 ay modern şifreleme yöntemleri ve akış şifreler konuları üzerine araştırma yapmıştır. 2014 yılında Bilgisayar/Bilişim Bilimleri ve Mühendisliği, Bilgi Güvenliği ve Kriptoloji alt alanında doçent ünvanını almıştır. Doç. Dr. Muharrem Tolga Sakallı, Siber güvenlik için uygulamalı kriptografi ve simetrik anahtarlı şifreleme teknikleri üzerine çalışmalarını sürdürmektedir. 1 patenti, çok sayıda ulusal ve uluslararası makale ve bildirisi bulunmaktadır.

Halen; Trakya Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanlığı görevini yürütmektedir.

Arş. Gör. Kübra SEYHAN

- Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü Araştırma Görevlisi, Samsun

Gümüşhane doğumlu olan Seyhan, 2013 yılında Gebze Yüksek Teknoloji Enstitüsü'nde başladığı lisans eğitimini 2016 yılında Karadeniz Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü'nde tamamlamıştır. 2017 yılında Ondokuz Mayıs Üniversitesi Bilgisayar Mühendisliği Bölümü'nde yüksek lisans eğitimine başlamıştır. İlgi alanları kuantum sonrası kriptografi ve bilgi güvenliği için uygulamalı kriptografi alanlarını kapsamaktadır. TÜBİTAK tarafından desteklenen bir projede bursiyer olarak görev yapmaktadır.

Arş. Gör. Meryem SOYSALDI

- Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü Araştırma Görevlisi, Samsun

Nevşehir doğumlu olan Soysaldı, 2013 yılında Fırat Üniversitesi Bilgisayar Mühendisliği Bölümü'nde lisans eğitimini tamamlamıştır.

Öğretim Üyesi Yetiştirme Programı kapsamında 2018 yılında Ondokuz Mayıs Üniversitesi Bilgisayar Mühendisliği Bölümü'nde yüksek lisans eğitimini tamamlamış ve sonrasında Ondokuz Mayıs Üniversitesi Hesaplamalı Bilimler Anabilim Dalı'nda doktora çalışmalarına başlamıştır. Kuantum sonrası kriptografi ve bilgi güvenliği için uygulamalı kriptografi alanlarında çalışmalarını sürdürmektedir. TÜBİTAK tarafından desteklenen iki projede bursiyer olarak görev yapmaktadır.

Mustafa ŞENOL

- E. Tuğgeneral, Doktor adayı, İTÜ Bilişim Enstitüsü Bilgi Güvenliği Mühendisliği ve Kriptografi Programı, İstanbul.

- HAVELSAN Yönetim Kurulu Başkan Vekili, Ankara.

Kocaeli doğumlu olan Mustafa Şenol; 1977 yılında Kuleli Askeri Lisesi'nden sonra 1981 yılında Kara Harp Okulu (Elektrik-Elektronik Mühendisliği Bölümü)'ndan Muhabere Teğmen olarak mezun olmuştur. 1982 yılında Muhabere (MEBS) Okulu'nu bitirdikten sonra Kara Kuvvetlerine ve Genel Kurmay Başkanlığına bağlı birlik ve karargâhlarda çeşitli görevlerde bulunmuştur.

1991-1992 yıllarında A.B.D.'de Muhabere, Elektronik Bilgi Sistemleri ve Haberleşme Eğitimi görmüş, "IBM Bilgisayarları Oryantasyonu", "Bilgisayar Programlama" ve "İleri Seviye Amerikan İngilizcesi" konularında eğitimler almıştır

Kara Harp ve Silahlı Kuvvetler Akademisi eğitimlerinin ardından tabur / alay komutanlıkları ve karargâh görevleri ile Askerî Ataşelik gö-

revi sonrasında 2009 yılında Tuğgeneralliğe terfi etmiş, iki yıl Tugay Komutanlığı görevinden sonra 2011 yılında Kara Kuvvetleri Muhabere Elektronik ve Bilgi Sistemleri (MEBS) Başkanlığı görevine atanmıştır.

Üç yıl süreli K.K.MEBS Bşk.lığı görevi sırasında Milli Güvenlik Akademisi'ni bitirmiş ve 30 Ağustos 2014 tarihinden itibaren, 40 yıllık askerlik yaşamından sonra kadrosuzluk nedeniyle emekli olmuştur.

2015-2017 yıllarında İstanbul Teknik Üniversitesi Bilişim Enstitüsü'nde "Bilgi Güvenliği Mühendisliği ve Kriptografi" programında Doktora eğitimi görmüş olup sırasıyla; "Siber Savaş (2012)", "Atatürk'ün Askerlik ve Liderlik Anlayışı (2016)", "Siber Güçle Caydırıcılık Ama Nasıl? (2017)", "Ulusal Siber Güvenlik Stratejisi Oluşturma ve Uygulama İçin Bir Yaklaşım", "Türkiye'de Siber Saldırılara Karşı Caydırıcılık (2017)" ve "Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık (2018)" konularında yayımlanmış makaleleri ile "Siber Terörizme Karşı Siber Savunma ve Caydırıcılık (2012)" konusunda Milli Güvenlik Akademisi için hazırlanan bir incelemesi bulunmaktadır. Ayrıca, Prof. Dr. Eşref Adalı tarafından yazılan; Bilgisayar ve Bilgi Güvenliği ve Yönetimi (2016) ve Bilişim Etiği ve Hukuku (2017) kitaplarının hazırlanmasında bulunmuş ve katkılar sunmuştur.

2017-2018 yıllarında bir yıl süreli TSK Mehmetçik Vakfı Genel Müdür Yardımcılığı görevinde bulunmuş olan E.Tuğg. Mustafa Şenol, halen 03 Mayıs 2018'de atanmış olduğu HAVELSAN-Hava Elektronik ve Ticaret Sanayi AŞ'nin Yönetim Kurulu Başkan Vekilliği görevini yürütmekte ve "Siber Güvenlik Stratejisi ve Caydırıcılık" konusundaki Doktora tez çalışmalarına devam etmektedir.

Dr. Adem TEKEREK

Dr. Adem Tekerek, Kahramanmaraş'ta doğmuştur. 2007 yılında Gazi Üniversitesi Teknik Eğitim Fakültesi, Elektronik Bilgisayar Eğitim Bölümünden Lisans, 2010 yılında Gazi Üniversitesi Bilişim Enstitüsü, Elektronik Bilgisayar Eğitimi Anabilim Dalından Yüksek Lisans ve 2016 yılında Gazi Üniversitesi, Bilişim Enstitüsü Elektronik Bilgisayar Eğitimi Anabilim Dalından Doktora derecelerini almıştır. Halen Gazi Üniversitesi Bilgi İşlem Daire Başkanlığında öğretim görevlisi olarak görev yapmakta-

dır. Yapay sinir ağları, derin öğrenme, veri madenciliği alanların çalışmaları bulunmaktadır. Web Güvenliği, Siber Güvenlik, Büyük Veri, Nesnelerin İnterneti alanlarında araştırma ve çalışmalarına devam etmektedir. Ulusal ve uluslararası birçok konferans ve dergide bilimsel yayınları bulunmaktadır.

Hatice TOMBUL

- TÜBİTAK SAGE Uzman Araştırmacı, Ankara

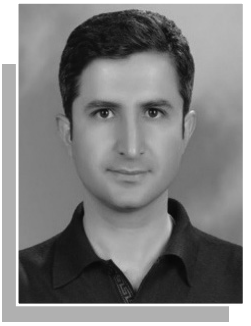
2009 yılında TOBB Ekonomi ve Teknoloji Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünden lisans, 2013 yılında ise aynı üniversitenin Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği bölümünden yüksek lisans derecelerini almıştır. 2014 yılından beri Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünde doktora çalışmalarına devam etmektedir. 2011-2019 yılları arasında Başkent Üniversitesi Bilgisayar Mühendisliği Bölümünde Araştırma Görevlisi olarak çalışmıştır. 2019 yılında üniversitedeki bu görevinden ayrılarak TÜBİTAK SAGE'de Uzman Araştırmacı olarak çalışmaya başlamıştır. Makine öğrenmesi, sinyal işleme konularında çalışmalarına devam eden Tombul, bilgi güvenliği ve siber güvenlik konularına ilgi duymaktadır.

Mehmet TUNÇKANAT

- IBM Müşteri İnovasyon Merkezi Müdürü

Yaklaşık 20 yıldır bilişim sektöründe tecrübeleri olan Mehmet Tunçkanat, IBM Müşteri Inovasyon Merkezi Müdürü olarak görev yapmaktadır. Akademide ve global teknoloji şirketlerinde Araştırma, Yazılım, Program Yönetimi ve Ürün Müdürlüğü alanlarında çalışmıştır.

Son dönemde özellikle ilgilendiği konular arasında Yapay Zekâ, Endüstri 4.0, dijital dönüşüm ve sibergüvenlik konuları yer almaktadır. Bilgisayar Mühendisliği lisans ve yüksek lisans dereceleri sahibidir.



Dr. Mehmet Rida TÜR

- Mardin Artuklu Üniversitesi Midyat Meslek Yüksekokulu Elektrik ve Enerji Dr. Öğretim Görevlisi. Bölüm Başkanı.

2010-2019 yılları arasında Elektrik ve Enerji Bölümünde Bölüm başkanlığı yapmıştır. Güç Sistemleri ve Şebeke Uygulamaları ile Üretim Sistemleri ve Şebeke Bağlantıları alanlarında dersler vermektedir. Güç sistemlerinde güvenirlik, koruma, enerji ekonomisi ve enerji kalitesi konularında çalışmalar yapmaktadır. Yayınlanmış bir kitap ve iki kitap bölümü bulunmaktadır. Bu çalışmalardan sonuncusu "Türkiye'de Elektrik Enerjisi" olup açık kaynak olarak okuyuculara sunulmaktadır. 80'nin üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi, ulusal ve uluslararası yayımlanmış bildirisi ile atıfları bulunmaktadır. ICRERA 2015-2018 konferanslarında komite üyesi olarak görev yapmış.

Teknoloji ve Tasarım alanında bir akademik derginin de alan editörlüğünü, birçok ulusal ve uluslararası Science Citation Index/Expanded ve TR dizinli dergilerde de hakemlik yapmaktadır. Kapasite Mekanizması, Ulusal güç sisteminin altyapısı geliştirmeye yönelik akıllı şebeke gereksinimleri, şebeke entegrasyonu problemi ve siber güvenlik konusunda çalışmaları devam etmektedir. IEEE üyesidir.

Öğr. Gör. Seyfettin VADİ

Gazi Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, Elektronik ve Otomasyon Bölümünde öğretim görevlisi olarak çalışan ve Kırıkkale doğumlu olan Vadi, 2009 yılında lisans eğitimini Gazi Üniversitesinde tamamladı. 2014 yılında, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik Eğitimi Anabilim Dalında, "Senkron Motor ile Reaktif Güç Kompanzasyonu için Web Tabanlı bir Eğitim Aracı" konulu bir tez hazırlayarak Yüksek Lisans derecesi aldı. Doktora eğitimine ise 2017 yılında Gazi Üniversitesi'nde başladı ve halen devam etmektedir.

Otomasyon ve SCADA Sistemleri, güç sistemleri ve dağıtık üretimde optimizasyon ve kontrol konularında çalışmalar yapmaktadır. Yayın-

lanmış bir kitabı bulunmaktadır. 20'nin üzerinde ulusal ve uluslararası indeksli dergilerde yayınlanmış makalesi, ulusal ve uluslararası yayımlanmış bildirisi ile atıfları bulunmaktadır. Mikro şebekelerde geçiş kararlılığı, evirici ve dönüştürücü topolojileri konularında çalışmaları devam etmektedir.

Dr. Yılmaz VURAL

Kişisel Verileri Koruma Kurumu, Daire Başkanı, Ankara

Dr. Yılmaz Vural, 1974 yılında Kahramanmaraş'ta doğmuştur. Trakya Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümünden Lisans, Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalından Yüksek Lisans ve Hacettepe Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalından Doktora derecelerini almıştır. 20 yılın üzerinde sektör tecrübesine sahip olan Dr. Vural Hacettepe Üniversitesi Bilişim Enstitüsü ve Gazi Üniversitesi Bilgisayar Mühendisliği bölümlerinde Bilgi Güvenliği, Bilgisayar Ağları, Veri Mahremiyeti konularında lisans ve lisansüstü, derslerini vermektedir. Halen Kişisel Verileri Koruma Kurumu Veri Güvenliği ve Bilgi Sistemleri Daire Başkanı olarak görev yapmaktadır.

Dr Vural Veri Mahremiyeti, Siber Güvenlik, Büyük Veri, Nesnelerin İnterneti alanlarında araştırma ve çalışmalarına devam etmektedir. Ulusal ve uluslararası birçok konferans ve dergide bilimsel yayınları bulunmaktadır.

Bilgi Güvenliği Derneği, kuruluşundan bugüne kadar ülkemizin "**Siber Güvenlik ve Savunmasının**" gelişimine katkı sağlamakta, birikimini topluma aktarmakta, içerik üretilmesine, yeni çözümler geliştirilmesine ve bilginin yaygınlaştırılmasına destek vermekte, kamuoyunun farkındalığını artırmaya çalışmakta, ve sonuçta siber ve bilgi güvenliğinin kişisel, kurumsal ve ulusal boyutta sağlanmasına katkılar sunmaktadır.

Tehditlerin artması, boyut ve yön değiştirmesi, çeşitlerinin artması, siber tehdit ekosisteminin büyümesi, kritik altyapıların hedef haline gelmesi, bilgi hırsızlıklarının çoğalması, yeraltında çalışan konsanların etkinleşmesi, siber tehditlerin artık savaşa dönüşmesi, siber suçların ve suçluların çoğalması, siber terörün artması nedeniyle, siber saldırılarla, suçlarla, terörizmle, zafiyetlerle mücadeleye her zamankinden daha fazla ihtiyaç duyulmaktadır. Kapsamlı bir mücadele için; ulusal stratejileri ve eylem planlarının hayata geçirilmesi, etkili araştırma merkezlerinin açılması, yeni altyapılar kurulması, yeni programların açılması ve son zamanlarda ise "siber ordular", "mükemmelliyet merkezleri", "ulusal siber olaylara müdahale", "siber savunma ajansı" gibi yapıların kurulması, vb. ihtiyaçlar bizleri bu kitap serisini hazırlamaya yöneltmiştir. Tehditlerin boyutunu ve geleceğini anlamak ancak ve ancak bu alanın kapsamını iyi anlamak, gelecekte karşılaşılacak olan tehditleri öngörmek, buna hazır olmak için konunun etkileşim içerisinde olduğu tüm alanları iyi bilmek, etkileşim içerisinde olunan alanları iyi tanımak, yeni alanları öğrenmek gerekmektedir. Siber güvenlik ve savunmaya kapsamlı bir bakış sunmayı amaçlayan bu eser serisinin, ülke siber güvenliğimiz ve savunmasına katkı sağlaması beklenmektedir.

HAVELSAN Bu kitap HAVELSAN'nın katkılarıyla basılmıştır.

ISBN : 978-605-2233-50-4

9 786052 233504

grafiker.com.tr • 0 312. 284 16 39