Türkiye'de Siber Saldırı Olayları ve Siber Savunma Yeteneklerinin Gelişimi¹

Sertan Akçalı

ORCID ID: <https://orcid.org/0000-0002-9912-3590>

Milli Savunma Üniversitesi, Barbaros Deniz Bilimleri ve Mühendisliği Enstitüsü, İstanbul – TÜRKİYE

Öğr. Gör. Dr. Mehmet Bilge Kağan Önaçan

ORCID ID: <https://orcid.org/0000-0002-7147-0945>

Milli Savunma Üniversitesi, Barbaros Deniz Bilimleri ve Mühendisliği Enstitüsü, İstanbul – TÜRKİYE

Makale Geçmişi

Geliş: 29.11.2019

Kabul: 29.12.2019

On-line Yayın: 31.12.2019

Anahtar Kelimeler

Siber Güvenlik

Siber Saldırı

Siber Uzay

Bilişim Teknolojileri

Güvenlik

Siber Tehdit

Önlemler

Araştırma Makalesi

DOI: [10.9761/JASSS40409](https://doi.org/10.9761/JASSS40409)

Öz

İnsanoğlunun var oluşundan beri yaşamın en temel ihtiyaçlarından biri olan güvenlik; insan, insan toplulukları ve bu toplulukların oluşturduğu devletlerin var olması, varlığını sürdürebilmesi açısından hayati öneme sahiptir. Her dönemin gereksinimlerine göre şekillenen güvenlik, yaşadığımız çağda bilişim teknolojileri ve bu teknolojilerin her alana nüfuz etmesiyle yeni bir boyut kazanmıştır. Bu teknolojiler çağımızda bilgisayar, cep telefonu ve internet gibi materyallerin kullanımının yaygınlaşmasıyla “Siber Uzay” olarak tabir edilen ortamı oluşturmuştur. Bu ortam sağladığı kullanım faydalarının yanı sıra pek çok güvenlik açıklarını da barındırmaktadır. Bu güvenlik açıklarının oluşturduğu riskler ve tehditler kişilerden, devletlerin güvenliğine kadar her boyutta meydana gelebilmektedir. Önceleri daha çok kişileri hedef alarak yapılan siber saldırılar, devlet kurumları ve özel kurumların da bu teknolojileri gün geçtikçe daha yoğun kullanmaları nedeniyle hedef alanını genişletmiştir. Özellikle bir kamu kurumunun siber saldırıya uğraması sonucu oluşabilecek zararların boyutu çok daha büyük olmaktadır. Bu etkilerinden dolayı devletler, tehlikeleri öngören ve engelleyen birtakım önlemler almak zorundadır. Bunun için de daha önce meydana gelmiş olayların tespiti, analizi ve değerlendirilmesi büyük öneme sahiptir. Buradan hareketle bu kavramsal çalışmada açık kaynak verileri derlenerek yakın dönemde Türkiye’de kamu kurum ve kuruluşlarına yönelik gerçekleşen siber saldırılar, saldırılara karşı alınan tedbirler ve saldırıların ulusal güvenliğe etkilerinin değerlendirilmesi amaçlanmaktadır. Çalışma sonunda görülmüştür ki Türkiye yoğun siber saldırıya maruz kalan ülkelerden biridir ve dolayısıyla siber savunmaya önem vererek bu alandaki yeteneklerini geliştirmeyi sürdürmesi gerekmektedir.

Atıf Bilgisi / Reference Information

Akçalı, S. ve Önaçan, M. B. K. (2019). Türkiye’de Siber Saldırı Olayları ve Siber Savunma Yeteneklerinin Gelişimi. *Jass Studies- The Journal of Academic Social Science Studies*, Number: 78, Winter, p. 21-37.

¹ Bu makale, 24-25 Ekim 2019 tarihlerinde İstanbul’da yapılan 1. Uluslararası Şişli Bilim Kongresi’nde sunulan bildirinin genişletilmiş ve güncellenmiş halidir.

Cyber Attack Incidents and Developments of Cyber Defence Capabilities in Turkey

Sertan Akçali

National Defense University, Barbaros Naval Sciences and Engineering Institute, Istanbul – TURKEY

Lect. Mehmet Bilge Kağan Önaçan, Ph.D

National Defense University, Barbaros Naval Sciences and Engineering Institute, Istanbul – TURKEY

Article History

Submitted: 29.11.2019

Accepted: 29.12.2019

Published Online: 31.12.2019

Key Words

Cyber Security

Cyber Attack

Cyber Space

Information Technologies

Security

Cyber Threat

Measures

Research ArticleDOI: [10.9761/JASSS40409](https://doi.org/10.9761/JASSS40409)**Abstract**

Security, which has been one of the most basic needs of life since the existence of human beings; has vital importance with regards to the existence of people, human communities and the states. Security, which is shaped according to the requirements of each era, has gained a new dimension in our era with the effect of information and communication Technologies (ICT). These technologies have created the dimension which is called "Cyber Space". In addition to the benefits, this dimension also has many security vulnerabilities. The risks and threats posed by these vulnerabilities can occur in any environment, from the security of individuals to the security of states. Cyber attacks, targeting individuals at the begin, have expanded its target area to the public institutions of the states due to the increasing use of ICT by states. In particular, the cyber attack to a public institution can cause significant damage. Because of the significant effects of cyber attacks, states have to take measures to foresee and prevent these attacks. For this, it is important to detect, analyze and evaluate the cyber attack events that have occurred before. From this point of view, this conceptual study aims to evaluate cyber attacks, measures taken against these attacks and their effects on national security. At the end of this study, it was determined that Turkey was one of the countries exposed to the intense cyber attacks and therefore, she should continue to develop its capabilities on cyber defence.

Giriş

Günümüzde internet kullanımı her geçen gün artmaktadır. Alışveriş, eğitim, bankacılık işlemleri, kamusal hizmetlere erişim gibi birçok kullanım kolaylığı sunan internet teknolojisi beraberinde riskler ve güvenlik açıklarını da getirmektedir. Bu riskler, dolandırıcılık faaliyetleri, sahtecilik, taciz ve şantaj gibi sadece kişiyi hedef almayıp, bir ülkenin haberleşme, enerji, ulaşım, finans, sağlık, gibi kritik altyapılarını, özel kuruluşların ticari sırlarını ve politikalarını da hedef almaktadır. Özellikle kamusal alanda hedef olabilecek unsurlardan biri veya birkaçında meydana gelebilecek aksaklık, ulusal anlamda birçok kayıp yaşanmasına sebep olabilmektedir.

Endüstri 4.0 ve kripto para ile birlikte insan hayatındaki birçok sürecin elektronik ortama aktarılması sonucu siber güvenlik ve siber savunma konularının gün geçtikçe daha önemli hale geleceği açıktır. Dolayısıyla siber güvenlik ve siber savunma konularında farkındalık yaratılması (Önačan ve Yıldırım, 2016), yaşanan olayların tespit edilerek bunlardan dersler çıkarılması ve sonraki dönemlerde önlemler alınması gerekmektedir.

Buradan hareketle bu kavramsal çalışmanın amacı; Türkiye’de siber savunma kapsamında alınan önlemlerin belirlenmesi, açık kaynaklardan elde edilen verilerin derlenerek yakın dönemde Türkiye’de kamu kurum ve kuruluşlarına yönelik gerçekleşen siber saldırıların, saldırılara karşı alınan tedbirlerin bir bütün halinde listelenmesi ve saldırıların ulusal güvenliğe etkilerinin değerlendirilerek öneriler sunulmasıdır. Bu kapsamda araştırmanın soruları aşağıdaki şekilde belirlenmiştir:

- Gelişen siber tehditler karşısında Türkiye’de siber savunmaya yönelik alınan tedbirler nelerdir?
- Türkiye’de yakın dönemde kamu kurum ve kuruluşlarına yapılan siber saldırılar ve etkileri nelerdir?
- Siber uzayda güvenliğin artırılmasına yönelik alınabilecek önlemler nelerdir?

Çalışmanın sonraki bölümlerinde siber uzaya ilişkin temel kavramlar, Türkiye’de siber uzaydaki faaliyetlerin yürütülmesinden sorumlu birimler, siber güvenlik stratejisi ve altyapı politikaları, Türkiye’de meydana gelen siber olaylar, doğrudan Türkiye’yi ve kurumlarını hedef alan siber saldırılar ve siber uzayda güvenliğin artırılmasına yönelik alınabilecek önlemlerden bahsedilmiş ve gelecek vizyonunu da içeren sonuç bölümüyle çalışma tamamlanmıştır.

SİBER UZAYA İLİŞKİN TEMEL KAVRAMLAR

Konunun daha iyi anlaşılması açısından öncelikle siber uzaya ilişkin temel kavramların burada kısaca açıklanmasının faydalı olacağı değerlendirilmektedir. Günümüzde süratle gelişen teknoloji, yarattığı kazanımlar ve sorunlar nedeniyle literatürümüze yeni bir boyut kazandırmıştır. Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan 2016-2023 Ulusal Siber Güvenlik Stratejisi’nde beşinci boyut olarak adlandırılan Siber Uzay, “Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamı” ifade etmektedir. Siber uzayda bir çeşit elektronik saldırı biçimi olan Siber Saldırı ise “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 işlemlerdir” (UDHB, t.y: 8). Bir başka ifadeyle siber saldırı. “Hedef seçilen birey, şirket, kurum, örgüt ve devlet gibi yapıların bilişim ve iletim sistemlerine, kritik yapılarına yapılan planlı ve koordineli saldırı(lar)dır” (Alkan, 2012). “Devletlerin birbirine karşı yürüttüğü siber saldırı faaliyetleri” (Çiftci, 2016: 6) ise Siber Savaş olarak tanımlanmaktadır. Bu savaş birçok boyutta yer almakta özellikle bir devletin hayati öneme sahip kurumları ve kritik altyapılarını hedef alarak önemli ölçüde hasara ve karışıklıklara sebep olabilmektedir. Bir ülkenin hayati öneme sahip kritik altyapıları, “Avrupa Komisyonu tarafından, zarar görmesi veya yok olması halinde,

vatandaşların sağlığına, emniyetine, güvenliğine ve ekonomik refahına veya kamu hizmetlerinin etkin ve verimli işleyişine ciddi boyutta olumsuz etki edebilecek fiziksel ve teknolojik tesisler, şebekeler, hizmetler ve varlıklar” (Ünver ve diğerleri, 2011) olarak tanımlanmaktadır. Bütün dijital işlemlerin gerçekleştiği siber uzayda oluşan tehditlerin bertaraf edilmesi, hem kişisel bilgisayarlar hem de kritik altyapıların saldırılardan korunabilmesi amacıyla birtakım güvenlik önlemlerinin alınması zorunlu hale gelmektedir. Bu kapsamda Siber Güvenlik; “Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmaların devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi” (USOM, 2014: 5) olarak tanımlanmaktadır. Siber güvenliğin sağlanmasına yönelik alınan tedbirlerin, Amerikalı siber savaş araştırmaları uzmanı Martin C. Libicki tarafından “siber ortamda saldırganın eylemini boşa çıkarma veya cezalandırma (misilleme tehdidi) yoluyla saldırıdan vazgeçirme” şeklinde tanımlanan (Şenol, 2017: 4) siber caydırıcılığa da etki ettiği değerlendirilmektedir. Kripto para ve şeylerin interneti (Internet of Things - IoT) gibi teknolojilerin (Kuru vd., 2019) gündelik hayatta daha yoğun kullanılmaya başlamasına bağlı olarak siber güvenliğin her geçen gün öneminin artması sebebiyle tüm dünyada olduğu gibi Türkiye’de de bir kısım tedbirler alınmakta, bu kapsamda yeni birimler oluşturulmaktadır. Sonraki bölümde Türkiye’de siber alandaki faaliyetlerin yürütülmesinden sorumlu birimler ile siber güvenlik stratejisi ve altyapı politikaları açıklanacaktır.

TÜRKİYE’DE SİBER UZAYDAKİ FAALİYETLERİN YÜRÜTÜLMESİNDEN SORUMLU BİRİMLER, SİBER GÜVENLİK STRATEJİSİ VE ALTYAPI POLİTİKALARI

Siber uzayda zaman ve mekan kavramı yoktur. Dolayısıyla zamandan ve mekandan bağımsız olarak gerçekleşen siber saldırılar, bilgisayar kontrollü cihazlar ve internet teknolojisinin hayatın her alanında yer almasıyla birlikte artmaktadır. Artan siber saldırıların verdikleri zararların sadece kişisel bilgisayarlar ile sınırlı olmayıp bir ülkenin kritik altyapı sistemlerine de önemli ölçüde tehdit oluşturması, devletlerin konuyla ilgili önlemler almasını zorunlu hale getirmiştir. Bu nedenle etkin sistemlerin oluşturulması, acil eylem planlarının hazırlanması, siber güvenlikle ilgili kurumlar oluşturularak bu kurumlara yetki ve sorumluluklar verilmesi, kamusal alanda farkındalık oluşturulması, uluslararası iş birliği faaliyetleri gibi önlemler tehlikenin oluşmadan yok edilmesi anlamında büyük önem arz etmektedir. NATO ve AB gibi uluslararası örgütler, ABD, Çin ve Rusya gibi bilişim teknolojilerinde gelişmiş olan ülkeler, olası bir siber saldırıya karşı alınacak önlemleri araştırmakta ve siber uzayda üstünlük sağlamaya çalışmaktadırlar. Ayrıca görevi, siber saldırılara anında cevap vermek ve düşmanın hayati öneme sahip bilgi teknolojilerini devre dışı bırakmak olan “siber ordular” oluşturmaktadırlar (Gürkaynak ve İren, 2011). Örneğin, Çin Halk Cumhuriyeti, kendisine yapılan siber saldırıları bertaraf etmek amacıyla 2011 yılında askerlerden ve üniversite öğrencilerinden oluşan “Mavi Ordu” adıyla siber savaş birimini kurduğunu açıklamıştır (Altun, 2017: 32).

Küresel gücün en önemli aktörü ABD’nin siber güvenlik politikaları incelendiğinde, bilişim teknolojilerindeki ilk adımları 1930’lu yıllarda attığı, 1990’lara gelindiğinde siber uzaydaki gelişmeleri fırsat olarak değerlendirdiği görülmüştür. Bu alanda önemli stratejiler geliştirerek siber alanda kapasitesini artırmış, siber uzaydaki siber gücünü artırmak maksadıyla kurum ve kuruluşlar oluşturmuştur (Darıcılı, 2017: 3).

Küresel gücün diğer önemli aktörlerinden biri olan Rusya da siber uzayın sunduğu fırsatları, yenilikleri kullanarak dış politikada hedeflerine ulaşma gayreti içindedir. Bu kapsamda 26 Aralık 1997’de yayımlanan Rusya Ulusal Güvenliği strateji belgesinde; askeri örgütlenmenin gelişen teknolojiyle revize edilmesi ve bilgi teknolojilerinin gelişimine atıfta bulunularak, bu teknolojilerin

artırılmasının hedeflendiği bildirilmiştir (Fas.Org., 1997).

Türkiye’de bilişim teknolojileri ile ilgili gelişmeler ve siber güvenlik faaliyetleri incelendiğinde, ilk yasal metnin, 1991 yılında Türk Ceza Kanunu’na eklenmiş olan “bilgileri otomatik işleme tutan sistem” ibaresi olduğu görülmektedir (BTK, 2016). Daha sonra 2004 yılında 5237 sayılı Ceza Kanununa bilişim suçları başlığı altına, sistemi engelleme, bozma, verileri yok etme değiştirme, banka kartlarının kötüye kullanılması, bilgisayar telekomünikasyon cihazları gibi bilişim sistemlerinin kullanılmasıyla işlenebilecek özel hayatın mahremiyeti, haberleşmenin engellenmesi, hırsızlık, dolandırıcılık, kumar ve sahtecilik gibi suçlar eklenmiştir (Bıçakçı vd., 2015). 2007 yılında ise 5651 sayılı “İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun” yürürlüğe girmiştir (Resmi Gazete, 2007).

Bunların yanı sıra bilgisayar ağları veya internet aracılığıyla işlenen suçlarla ilgili uluslararası bir sözleşme olan ve Strazburg’da Avrupa Konseyi ile imzalanan ‘Sanal Ortamda İşlenen Suçlar Sözleşmesi’, Türkiye’de 02 Mayıs 2014 tarihinde yürürlüğe konan 6533 sayılı kanun ile onaylanmıştır (Taşçı ve Can, 2015). Sonuç olarak, Türkiye’de bilişim alanında oluşturulan yasal düzenlemeler, genel olarak Avrupa Birliği (AB) direktiflerine uyumlu bir çerçevede hazırlanmıştır. Ayrıca Türkiye’de bilişim suçları tek bir kanunla belirlenmemiş, mevcut kanunlara ilgili hükümler eklenerek oluşturulmuştur (BTK, 2016). Bu gelişmelerle birlikte, Türkiye’de siber alandaki faaliyetlerin yürütülmesinden sorumlu birimlerin kurulması yönünde adımlar atılmıştır. Bu kapsamda üç temel amaca yönelik olarak siber güvenlik kurumları organize edilmiştir. İlk grup siber suçlar ile mücadele etmek ve faaliyet alanları dahilinde istihbari çalışmalarda bulunmak amaçlı kurumlardır (Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı bünyesindeki birimler). İkinci grup Türkiye’nin kritik altyapılarının siber güvenliğini sağlamak, siber savunma ve saldırı kapasitesini oluşturmak amaçlı kurumlardır (BTK, MİT, AFAD, TSK Siber Savunma Komutanlığı, TÜBİTAK gibi). Üçüncü grup ise devlet destekli özel girişimlerdir (STM, HAVELSAN, ASELSAN bünyesindeki birimler) (Darıcılı, 2019: 28). Sonraki bölümde Türkiye’nin siber alandaki faaliyetlerin yürütülmesinden sorumlu önemli birimlerden bazılarından bahsedilecektir.

TÜBİTAK (BİLGEM)

Ulusal siber güvenliğin sağlanması amacıyla 1997 yılında faaliyetlerine başlamıştır. İlk yıllarında Ağ güvenliği konularına odaklanarak ulusal savunmaya yönelik testler gerçekleştirmiştir. Kurum ilerleyen yıllarda dünyada önemli test merkezlerinden biri haline gelmiş, kriptoloji cihazları için haberleşme güvenliği testleri ve akıllı kart güvenliği çalışmalarını artırarak özellikle yan kanal analizi, tersine mühendislik konularında uzmanlık kazanmıştır. Bünyesinde bulunan Ağ Güvenliği Grubu, kuruluşundan günümüze kadar Türk Silahlı Kuvvetleri’nin bilişim sistemleri güvenliği alanındaki ihtiyaçlarını karşılamak üzere birçok proje gerçekleştirmiştir. Ayrıca özel sektörle de birlikte projeler yürüterek ülkenin siber güvenlik kapasitesinin artmasına önemli katkıda bulunmuştur (TÜBİTAK, 2019). TÜBİTAK, 2012 yılına kadar siber güvenlikle sorumlu kurum olmuş, bu yetkisini 3842 sayılı Bakanlar Kurulu Kararı ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB)’na devretmiştir.

Siber Güvenlik Kurulu

Bilgi toplumu politika, hedef ve stratejileri çerçevesinde, UDHB’nın teşkilat ve görevleri 26 Eylül 2011’de ‘655 Sayılı Kanun Hükmünde Kararname (KHK)’ ile yeniden düzenlenmiştir. Anılan KHK ile UDHB’ye “Siber güvenlik faaliyetleri ve hizmetlerine ilişkin kamu kurum ve kuruluşlarıyla gerekli iş birliği ve koordinasyonun sağlanmasına ilişkin usul ve esasları belirlemek ve gerekli düzenlemelerin yapılması” görevi verilmiştir (Resmi Gazete, 2011). ‘Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin’ 20 Ekim 2012 tarihli Bakanlar Kurulu kararı ile “Ulaştırma, Denizcilik ve Haberleşme (UDH) Bakanı başkanlığında; Dışişleri, İçişleri,

Milli Savunma, UDH Bakanlıkları müsteşarlarının yanı sıra, Kamu Düzeni ve Güvenliği Müsteşarı, MİT Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, BTK Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ve UDH tarafından belirlenen bakanlık ve kamu kurumu üst düzey yöneticilerinden” oluşan (BTK, 2017) Siber Güvenlik Kurulu oluşturulmuştur. “Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak, kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak, siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek” (BTK, 2017) görevi olan Kurulun ilk toplantısı 2012 yılında yapılmış, Ulusal Güvenlik Stratejisi ve 2013-2014 Eylem planı kabul edilmiştir. Bu eylem planında bilişim alanında kamu veya özel sektör tarafından işletilen kritik altyapıların, kamu kurum ve kuruluşlarınca sunulan hizmetlerin güvenliğine ait stratejik eylemler belirlenerek oluşabilecek risklerin en aza indirgenmesi hedeflenmiştir. Kurulun toplantısı sonucunda aşağıdaki kararlar alınmıştır (UDHB, 2013):

- Yasal Düzenlemelerin Yapılması
- Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi
- Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması
- Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi
- Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri
- Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi
- Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi

2013-2014 Eylem planında karşılaşılan güçlüklerin önüne geçilmesi ve yeni stratejiler oluşturulması amacıyla 2015 yılında kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarının temsilcileriyle (Ortak Akıl Platformu), UDHB nezdinde 2016-2019 Siber Güvenlik Stratejisi ve Eylem Planı hazırlanmıştır. Anılan Siber Güvenlik Stratejisi ve Eylem Planı’nda, siber tehditlere karşı korunma, siber güvenlik alanında iş gücünün artırılması, yerli siber güvenlik çözümlerinin geliştirilmesi ve siber güvenliğin milli güvenlik sistemlerine entegrasyonu gibi beş stratejik amaç doğrultusunda 41 eylemin hayata geçirilmesi planlanmaktadır (Demirel, 2016).

Bilgi Teknolojileri ve İletişim Kurumu (BTK)

2000 yılının başlarında kurulan Telekomünikasyon Kurumu, 2008 yılında “5809 sayılı Elektronik Haberleşme Kanunu” ile “Bilgi Teknolojileri ve İletişim Kurumu (BTK)” olarak yeniden adlandırılarak tekrar yapılandırılmıştır. UDHB’nca belirlenecek politika ve stratejilere uygun olarak telekomünikasyon sektörünü düzenleyen bu kurumun görevi; yetkilendirme, denetleme, ihtilaf çözümü, tüketici haklarının korunması, sektör rekabetinin düzenlenmesi, teknik yönergeler yayınlamak ve spektrum yönetimi ve izlenmesidir (Bıçakçı vd., 2015). Ayrıca 06 Şubat 2014 tarihinde yayımlanan 6518 sayılı kanun ile mevcut Elektronik Haberleşme Kanunu’na bazı maddeler eklenerek BTK’ya siber güvenlik ile ilgili aşağıdaki yeni görevler verilmiştir (BTK, 2017)

- Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi
- İzinsiz erişime karşı şebeke güvenliğinin sağlanması
- Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması
- Siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek şeklinde belirtilmiştir.

TSK Siber Savunma Komutanlığı

2012 yılında TSK bünyesinde Türkiye’nin siber ordusu olarak bilinen Siber Savunma Merkezi Başkanlığı kurulmuş, 2013 yılında ise bu Başkanlık, TSK Siber Savunma Komutanlığı’na

dönüştürülmüştür. Ülkeyi siber saldırılara karşı savunmayı amaçlayan birim, Genelkurmay Başkanlığı bünyesinde Savunma Bakanlığı, TÜBİTAK ve ODTÜ iş birliğinde görev yapacak özel bir birim şeklinde planlanmıştır. 7/24 esasına göre çalışan kurumun görevleri (Bıçakçı vd., 2016);

- TSK'nın siber savunmasını sağlamak,
- Siber olaylara müdahale etmek,
- Ulusal ve uluslararası organizasyonlar tarafından icra edilen tatbikatlara iştirak etmek,
- TSK personelini bilinçlendirme ve eğitim faaliyetlerini yürütmek,
- TSK tarafından kullanılan ağların siber güvenlik denetlemelerini ve testlerini yapmak

olarak belirlenmiştir.

Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı

Şubat 2013 senesinde siber suçlarla mücadele amacıyla EGM bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur. Kurumun görevleri (EGM, t.y.);

- Siber suçlarla mücadele etmek,
- Siber suçlar konusunda toplumda farkındalık oluşturmak,
- Siber suçlarla mücadele amacıyla uluslararası iş birliklerini artırmak,
- Ülkemize yönelik siber suç tehditlerini değerlendirmek,
- Siber suçlarla mücadelede alanında uzman personel yetiştirmek,
- Siber suçlarla mücadele kapasitesini artırmak olarak belirtilmiştir.

Ulusal Siber Olaylara Müdahale Merkezi (USOM)

USOM, 2014 yılında BTK bünyesinde kurulmuştur. Türkiye'nin siber güvenliğine karşı ortaya çıkan tehditlerin tespit edilerek, saldırıların ve olayların etkilerinin asgari seviyeye indirilmesi veya yok edilmesine yönelik önlemler alınması ve yandaşlarla paylaşılması amacıyla oluşturulmuş, siber ortamda 7/24 esasına göre çalışan bir merkezdir. Ayrıca kamu kurum ve kuruluşlarının siber saldırılara karşı farkındalığının oluşturulması ve hazırlığının artırılması faaliyetleri de görevleri arasında bulunmaktadır (USOM, t.y.).

Özetlemek gerekirse bilincin artması, maruz kalınan siber saldırılar, tüm dünyadaki temayüller sebebiyle Türkiye'de de siber güvenliğe ilişkin değişik çalışmalar yapılmaktadır. Bu çalışmalar; Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Yasal Çalışmalar, Siber Güvenlik Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar ve Çalıştaylar ve de TSK bünyesinde icra edilen faaliyetler ve oluşumlar şeklinde sayılabilmektedir (Öğün ve Kaya, 2013: 167). Sonraki bölümde, yukarıda sayılan çalışmaların yapılmasına sebep olan etkenlerden siber saldırılara ilişkin bilgiler sunulmaktadır.

TÜRKİYE'DE MEYDANA GELEN SİBER SALDIRILAR

Günümüzde toplumun ve ekonominin ayrılmaz bileşenleri olan bilişim teknolojileri, kalkınmaya önemli katkı sağlamakta ve kamu kurumlarında, özel sektörde ve kritik altyapı hizmetlerinde bu teknolojilerin kullanımı artarak devam etmektedir. Artan kullanımıyla birlikte bilişim sistemlerinde güvenlik, ulusal güvenliğin ve rekabet gücünün önemli bir bileşeni haline gelmiştir. Söz konusu bilişim sistemlerinde bulunan güvenlik zafiyetleri kamu düzeni sorunlarına, önemli derecede ekonomik zararlara, ulusal güvenliğin ihlali gibi birçok soruna yol açabilmektedir. Türkiye açısından değerlendirildiğinde, bulunmuş olduğu coğrafyada yer alan ülkelerdeki istikrarsızlıklar, politik sorunlar gibi nedenler ulusal güvenliği açısından, fiziksel tehditler ile beraber siber tehditleri ve siber saldırıları da her geçen gün arttırmaktadır.

UDH Bakanı Arslan: "Dünyanın en büyük teknoloji firmalarından birinin yaptığı araştırmaya göre, siber saldırıların dünyaya maliyeti yılda 500 milyar doların üzerinde. 2016'da fiziksel olduğu gibi siber dünyada da Türkiye'ye yönelik iç ve dış saldırılar arttı. Belirli büyüklüğün üstündeki hizmet dışı

bırakma saldırı sayısı 2014'te 209 iken 2015'te 7 kat artarak bin 477'ye, 2016'da ise 6 kat daha artarak 8 bin 560'a çıktı" açıklamasında bulunmuştur (Yenişafak, 2017). Güvenlik yazılım şirketi olan Trend Micro'nun araştırmasına göre, Türkiye'nin en fazla maruz kaldığı siber saldırı çeşitleri (Hürriyet, 2016):

- Fidyeye yazılımları
- Oltalama saldırıları
- Kredi kartı dolandırıcılıkları
- DDoS saldırıları
- Mobil tehditlerdir. Aşağıda anılan saldırılar açıklanmaktadır.

Fidyeye Yazılımları

Her geçen gün artan ve gelişen fidye yazılımları, bilgisayarlarda bulunan bütün dosyaları şifreleyerek kullanılmaz hale getiren yazılımlardır. Bu saldırıyı düzenleyen kişiler, dosyaların açılabilmesi için fidye talep etmektedirler (KASPERSKYLAB, 2016). Genel olarak fidye yazılımı saldırıları incelendiğinde eğitim, sağlık, finans gibi iş sürekliliğinin önemli olduğu sektörleri daha çok hedef aldıkları görülmektedir. Bitsight siber güvenlik şirketinin yayınladığı raporda, eğitim sektörüne yapılan fidye yazılımı saldırılarının, sağlık sektöründen 3 kat, finans sektöründen ise 10 kat daha fazla olduğu ifade edilmektedir. Yayımlanan raporda fidye yazılımı saldırısına uğrayan her 5 şirketten birinin fidye ödemeyi kabul ettiği belirtilmektedir (HÜRRİYET, 2019).

SonicWall Capture Threat Network şirketinin tespitlerine göre 2016 yılında kaydedilen 638 milyon fidye yazılım saldırısı olmuşken, 2017 yılında 183,6 milyon fidye yazılım saldırısı tespit edilmiştir. 2017 yılındaki tüm fidye yazılım saldırıları incelendiğinde %46'sı Amerika, %7'si Latin Amerika ülkeleri, %9'u Asya ülkeleri ve %38'i Avrupa ülkelerini hedef almıştır. Yine SonicWall Capture Threat Network şirketinin tespitlerine göre 2017'nin en etkili fidye yazılımları (SONICWALL, 2018);

- WannaCry
- Petya
- Bad Rabbit
- Cerber
- Nemucod olarak belirtilmiştir.

Dünyada birçok örneği bulunan fidye yazılımı saldırı türlerinin son örneklerinden biri Mayıs 2017'de gerçekleşen WanaCrypt0r 2.0 isimli fidye yazılımı saldırısıdır. Avast yazılım şirketinin raporuna göre dünya çapında eş zamanlı olarak başlayan ve aralarında Türkiye'nin de bulunduğu 74 ülkeye yayıldığı bilinen zararlı yazılımın, İngiltere'nin Ulusal Sağlık Sistemi, İspanya'nın önemli şirketlerinden Telefonica, Iberdrola ve Gas Natural, Rusya Acil Durum Bakanlığı ve Rusya'nın önemli şirketlerinden olan MegaFon'a bulaştığı belirtilmektedir (CNNTURK, 2017).

Kaspersky Lab'in yayınladığı Nisan 2016'dan Mart 2017'yi ve Nisan 2017'den Mart 2018'i kapsayan rapora göre fidye yazılımı saldırılarının dünya çapında önemli düzeyde azaldığı belirtilmiştir. Bu azalmanın sebepleri arasında fidye yazılımlarına yönelik ortaya koyulan güvenlik çözümleri, artan farkındalık ve bilinçlendirme faaliyetleri, talep edilen fidyelerin ödenmemesi gibi çeşitli nedenler bulunmaktadır. Yayımlanan raporda Türkiye'nin, 2016-2017 döneminde kullanıcı oranı fidye yazılımı saldırısına uğrayan en yüksek ülkeler listesinde ilk sırada yer aldığı, 2017-2018 döneminde bu durumun değiştiği, %3,22 oranla onuncu sırada olduğu belirtilmiştir (CHIPONLINE, 2018). Yine Kaspersky Lab'in yaptığı açıklamada Türkiye'de 2017 yılında yapılan fidye yazılımı saldırılarının yüzde 43'ünün özel sektöre yapıldığına dikkat çekilmiştir (KASPERSKYLAB, 2017). Trend Micro tarafından yayınlanan 2018 yılı Aralık ayı küresel siber saldırı raporuna göre ise fidye yazılım saldırıları dünyada azalırken, saldırıların yüzde 4'üne yakını Türkiye'de gerçekleşmiştir. Türkiye'nin bu oranla Avrupa kıtası fidye saldırılarında ilk sırada, dünyada altıncı sırada olduğu ifade edilmiştir (HABERTÜRK, 2019).

Önemli ölçüde bilgi ve para kayıplarına sebep olan fidye türü yazılımlar, bilgisiz, bilinçsiz ve dikkatsiz kullanıcılara yönelik olarak etkinliğini sürdürmektedir. Farkındalık oluşturularak kullanıcıların bilinçlendirilmesi, bu tür saldırılardan korunulmasını büyük oranda mümkün kılabilir.

Oltalama saldırıları

Oltalama saldırısı, genellikle bir kurumdan gönderilmiş gibi sahte e-posta mesajıyla karşıdaki kişinin hedef alınmasıdır. Hedef alınan kişi e-postasına tıkladığında yine sahte bir adrese yönlendirilmekte, bu sahte adres aracılığıyla kişinin bilgileri, şifreleri ele geçirilmektedir. Kısaca mağdurun hassas bilgilerinin ele geçirildiği bir tür sosyal mühendislik saldırısıdır (CUMHURİYET, 2016). Oltalama saldırısı tekniklerini beş alt grupta incelemek mümkündür (Hekim, 2015):

- Kandırmaca içerikli oltalama saldırılarında; kullanıcının, saldırgan tarafından gerçeğine çok benzeyen sahte bir web sayfasına yönlendirilerek, bilgilerini sisteme girmesi sağlanmakta ve sisteme bilgilerini giren kullanıcının verileri ele geçirilerek saldırgan tarafından kötü amaçlarla kullanılmaktadır.

- Zararlı yazılımlar aracılığıyla gerçekleştirilen oltalama saldırıları; sosyal mühendislik teknikleri kullanılarak, internetten ücretsiz olarak indirilip yüklenebilen programlar aracılığıyla veya bilgisayarda yüklü yazılımların açıklarından istifade edilerek kullanıcı bilgisayarına yüklenebilen zararlı bir yazılımı kullanıcının bilgisayarında çalıştırmasıyla gerçekleşmektedir.

- DNS temelli oltalama saldırıları (Pharming); kullanıcının internet adresi bulma, çözümleme sisteminin, sahte web sitelerine ya da sunucuya yönlendirilerek değiştirilmesidir.

- İçerik Enjeksiyonu (Content-Injection) oltalama saldırıları; bir kurum veya kuruluşun web sayfasında veya yazılımlarındaki açıkların kullanılmasıyla zararlı içerik yerleştirilmesidir.

- Ortadaki adam saldırıları; saldırganın, hem kullanıcı hem de kurumun web sitesinin yer aldığı iki bağlantı arasına konumlanarak her iki taraftan gelen verileri dinlemesidir.

Kaspersky Lab şirketinin açıklamasında 2017 yılında Irak ve Suudi Arabistan'da görülen Muddy Water saldırısının hedefinde Türkiye ile beraber, Ürdün, Azerbaycan, Mali, Avusturya, Rusya, İran ve Bahreyn'in de yer aldığı belirtilmiştir. Oltalama mesajlarının ofis dosyaları kullanılarak gönderildiği belirtilen saldırıda özellikle askeri kurumların, eğitim kurumlarının, Telekom şirketleri gibi kritik öneme haiz kurumların hedef alındığı belirtilmiştir (KasperskyLab, 2018).

2017 yılı Mart ayı başlarında kökeni Kuzey Kore olan siber suç örgütleri tarafından düzenlendiği tahmin edilen saldırıda Türkiye'nin finans kuruluşları hedef alınmıştır. McAfee siber güvenlik şirketinden Sherstobitoff (2019), Bankshot adıyla bilinen yazılımın güncelleştirilmiş bir versiyonunu kullanan saldırganların hedefinde finans kuruluşlarının olduğunu belirtmiştir. Bu saldırı, zararlı içerik barındıran bir Microsoft Word belgesi kullanılarak oltalama yöntemi ile gerçekleştirilmiştir. Araştırmacılar, saldırı sonucunda herhangi bir para kaybının yaşanmadığını belirtmiş, fakat bu saldırının daha sonraki zamanlarda gerçekleştirilmesi planlanan büyük çaplı bir saldırı için hazırlık olabileceğine dair uyarıda bulunmuşlardır. McAfee uzmanları, 2019 yılı Bankshot virüsünün yeni sürümlerinin ortaya çıktığı ilk saldırının Türkiye'ye gerçekleştirildiğine dikkat çekmiştir.

Kredi kartı dolandırıcılıkları

Kredi kartı dolandırıcılıkları, genellikle kişinin kimlik bilgilerinin internet veya çeşitli dolandırıcılık yöntemleriyle ele geçirilmesi ve yeni bir kredi kartı çıkartılarak harcama yapılması veya doğrudan kredi kartı bilgilerinin ele geçirilmesiyle karttan harcama yapılması şeklinde gerçekleşmektedir (Yılmaz, 2015). Saldırganlar, özellikle internetten alışverişin yoğun olduğu anneler günü, sevgililer günü gibi yılın özel günlerinde kullanıcıları çeşitli kampanyalar, fırsatlar ve indirimler içeren sahte sipariş sayfalarına e-postalar aracılığıyla yönlendirmektedir. Bu e-posta adresine tıklayıp

alışverişini yapan kişinin kredi kartı bilgisi saldırganın eline geçmektedir (HÜRRİYET, 2016).

Türkiye, 2018 sonu itibarıyla 66 milyonu kredi kartı ve 148 milyonu da banka kartı olmak üzere 214 milyon kart ile son 5 yıldır Almanya ve İngiltere’nin de önünde Avrupa’da birinci, dünyada ise sekizinci sırada yer almaktadır (tr.sputniknews.com, 2019). Kredi kartı ve banka kartı kullanımı çoğaldıkça, dolandırıcılık yöntemleri ve dolandırıcılığına maruz kalanların sayısı da her geçen gün artmaktadır. Türkiye’de son beş yılda kredi kartı dolandırıcılığına maruz kalarak mahkemelere başvuran kişi sayısının beş yüz bini geçmiş olduğu ayrıca her yıl yaklaşık olarak yüz bin kişinin dolandırıcılığa maruz kaldığı belirtilmektedir (TAKVİM, 2019). Trend Micro’nun araştırmasına göre Türkiye’de online bankacılığa yönelik tehditler de artmaktadır. Rapora göre Türkiye 11 bin 516 saldırı ile Avrupa’da en fazla online bankacılık saldırısının yapıldığı ülke durumunda bulunmaktadır (STM, 2016).

Denial of Service (DoS) ve Distributed Denial of Service Attack (DDoS) Saldırıları

Son dönemde ülkemizin gündemini meşgul eden siber saldırıların başında DoS ve DDoS saldırıları gelmektedir. DoS saldırıları, hedef sisteme cevap veremeyeceği kadar istek gönderilerek sistemin yavaşlatılmasıdır. DDoS saldırıları ise, bir web sitesini veya ağ kaynağını kullanılamaz duruma getirmek maksadıyla birden fazla noktadan eş zamanlı olarak hedef sisteme istekler gönderilmesidir. DoS saldırılarında, saldırının tek kaynaktan olması nedeniyle önlenmesi kolaydır. Fakat dağınık bir saldırı tekniği olarak DDoS saldırısı yüzlerce, binlerce sistem kullanılarak gerçekleşmesi nedeniyle engellenmesi zor bir saldırı türüdür (Altınkaynak, 2017: 199-200).

Türkiye’de Türk Hava Yolları (THY) çalışanlarının grevlerine destek olmak amacıyla dünyaca ünlü hacker grubu Anonymous tarafından 2012 yılında gerçekleştirilen DDos saldırısında THY’nin resmi internet sitesi kesintiye uğratılmıştır. Saldırı sonucunda bilet satış işlemleri online yapılamazken, uçuşlar da gecikmiştir. Dünyada tanınırlığı yüksek olan THY’nin internet sitesine bilet almak için binlerce yolcunun girememesi sonucunda kurumun zararının 400 bin TL olduğu tahmin edilmektedir. Bununla beraber 6 saat süren saldırıda Türkiye’de en çok kullanılan 176 siteye de giriş engellenmiştir (MİLLİYET, 2012).

Türkiye 2015 yılının 14-24 Aralık tarihleri arasında büyük siber saldırılara maruz kalmıştır. Anonymous tarafından üstlenilen saldırılar sonucunda “.tr” uzantılı adreslere erişim sağlanamamış ya da sitelere girişlerde sorunlar yaşanmıştır. Genellikle 8 Gbps civarındaki DDoS saldırıları ciddi saldırılar olarak kabul edilirken, Türkiye 40 Gbps büyüklüklerinde saldırılar yaşamıştır. Türkiye’nin finansal altyapısını da hedef alan DDoS saldırılarında özellikle Garanti Bankası, Ziraat Bankası, İş Bankası ve Akbank’ın online bankacılık hizmetlerinde aksamalar yaşanmıştır (AHABER, 2015).

İzmir’deki doğal gaz dağıtım ve tedarikini sağlayan İzmir Gaz firmasının internet sitesi, 2016 yılı temmuz ayının ikinci yarısındaki Anonymous hacker grubunun #opTurkey adındaki siber saldırısı nedeniyle erişime kapatılarak bir süreliğine servis dışı bırakılmıştır. Yapılan saldırı ile şirketin veri tabanında yer alan kullanıcıların şifreleri, şirkete ait bütçe ve bakım raporları, üye detayları, faturalama bilgileri ele geçirilmiştir (STM, 2016).

Akamai firmasının 2017 yılının ikinci çeyreğinde hazırladığı raporuna göre, Türkiye DDoS saldırılarına kaynak ülkeler sıralamasında dünyada üçüncü sırada yer almaktadır. Saldırıların %32’sinin Mısır’a, %8’inin A.B.D’ ne, %5’inin Türkiye’ye yapıldığı belirtilmektedir (AKAMAI, 2017). Bir diğer siber güvenlik firması Radore’nin hazırladığı raporda, 2017 yılının ikinci çeyreğinden itibaren DDoS saldırılarının tüm dünyada arttığı, ayrıca saldırıya maruz kalanların yüzde 60’ından fazlasına yapılan saldırıların tekrarlandığı açıklanmaktadır (HÜRRİYET, 2018).

Mobil tehditler

İnternet ile bağlantılı olarak mobil cihazların kullanımlarının artmasından dolayı birçok zararlı yazılım mobil cihazlara indirilmektedir. TrendLabs tarafından yapılan araştırmada Türkiye’de 2015’in

üçüncü çeyreğinde zararlı ve yüksek tehlike içeren mobil uygulamaların 160 bin 717 kez kullanıcılar tarafından telefonlara indirildiği tespit edilmiştir (HÜRRİYET, 2016).

2017 yılında Antivirüs yazılım kuruluşu olan ESET, bir hava durumu uygulamasında mobil bankacılık işlemlerini hedef alan bir virüs tespit etmiştir. Kuruluş tarafından yapılan açıklamaya göre android platformu olan Google play’den “Good Weather” adıyla indirilen bu yazılım bulaştığı cihazın SMS mesajlarına erişebilmekte, cihazı kilitleyebilmekte ve mobil bankacılık bilgilerini çalabilmektedir. Açıklamada, bu zararlı yazılımın 48 ülkede 5 bin kullanıcıya ulaştığı ve 2 bin 144 indirme ile ülkemizin ön plana çıktığı duyurulmuştur. Yapılan analizler, yazılımın 22 Türk mobil bankacılık uygulamasını hedef aldığını göstermiştir (ESET, 2017). Kaspersky Lab Güney Afrika’ da düzenlenen Cyber Security Weekend etkinliğinde, Orta Doğu, Türkiye ve Afrika (Meadle East, Turkey and Africa- META) bölgesinde ülkemizin, mobil zararlı yazılım ve kimlik avı saldırısı kategorilerinde birinci sırada yer aldığını belirtmiştir (CUMHURİYET, 2019).

DOĞRUDAN TÜRKİYEYİ VE KURUMLARINI HEDEF ALAN BAZI SİBER SALDIRILAR

Dünyanın birçok ülkesinde olduğu gibi Türkiye de siber saldırıların hedefinde olan bir ülkedir. Türkiye’de bireyler, özel sektör kuruluşları ve devlet kurumları siber saldırılara maruz kalmaktadır. Bu saldırıların temel sebebinin Türkiye’nin içinde bulunduğu siyasi ve coğrafi yapı olduğu söylenebilir. Bir kısım ülke ve grupların siber saldırılar ile Türkiye’ye bazı yaptırımlar uygulamaya çalıştıkları veya zarar verme gayreti içinde oldukları görülmektedir. Bu kapsamda finans sektörü, maddi gelir elde etmeye yönelik saldırılara hedef olmaktadır. Bununla birlikte Avrupa ve Orta Doğu arasında enerji köprüsü olması sebebiyle enerji sektörü de siber saldırılara maruz kalmaktadır. Aşağıda Türkiye’yi doğrudan hedef alan bazı siber saldırı örnekleri sunulmaktadır.

RedHack, 1997 yılında kurulan Marksist ve sosyalist eğilimli grup, sivil direniş konusunda ülkemizdeki eylemler ve olaylarla ilgili çeşitli bilgi, video, fotoğraf ve yorumu hem ulusal kamuoyuna hem de uluslararası kamuoyuna duyurmak amacıyla İngilizce ve Türkçe olarak yayınlamaktadır. Ülkemize yönelik gerçekleşmiş pek çok saldırının arkasında olduğu düşünülen grubun Tablo-1’de belirtilen eylemleri sonucunda RedHack üyelerine karşı geniş çapta operasyonlar yapılmış ve üyeler birçok hukuki işlemlerle karşı karşıya kalmıştır (Yegen, 2014).

Tablo-1 Redhack grubu tarafından ülkemizi hedef alan saldırılar (Turak, 2014).

Tarih	Hedef Alınan Kurum	Etkileri
27 Şubat 2012	Ankara Emniyet Genel Müdürlüğü	Ankara Emniyet Genel Müdürlüğü’nün internet sitesinin çökertilmesi ve çok sayıda ihbar ve iç yazışmanın internet ortamında yayınlanması.
20 Nisan 2012	İçişleri Bakanlığı	İçişleri Bakanlığı sitesine ait bir alt sayfaya mesaj bırakılması.
27 Nisan 2012	TTNET	İnternet hizmetinin yaklaşık 2 saat süreyle aksatılması.
2 Mayıs 2012	K.K.K.’lığı	Bazı TSK personelinin bilgilerinin ifşa edilmesi.
14 Mayıs 2012	Aile ve Sosyal Politikalar Bakanlığı	Kurumun internet sitesinin hacklenmesi.
29 Mayıs 2012	THY	Kurumun internet sitesine saldırı

		düzenlenmesi.
03 Temmuz 2012	Dışişleri Bakanlığı	Kurumun dosya paylaşım sitesi hedef alınarak, Türkiye’de çalışan birçok yabancı diplomatın kimlik bilgilerinin Dropbox üzerinden yayınlanması.
16 Temmuz 2012	Ankara Emniyet Genel Müdürlüğü	İhbarların bulunduğu .txt uzantılı dosyaların yayınlanması.
29 Ekim 2012	Diyanet İşleri Başkanlığı	Kurumun internet sayfasının hacklenmesi.
07 Aralık 2012	Maliye Bakanlığı	Kurumun internet sayfasının hacklenmesi.
08 Ocak 2013	Yüksek Öğrenim Kurumu	Kurumun internet sayfası hacklenerek bazı belgelerin yayınlanması.
26 Şubat 2013	Ankara Büyükşehir Belediye Başkanı	Dönemin Ankara Büyükşehir Belediye Başkanı hakkında belgelerin yayınlanması.
22 Mart 2013	Ankara Büyükşehir Belediyesi	Kurumun internet sayfasının hacklenmesi.
05 Mayıs 2013	İstanbul Valiliği	Kurumun internet sayfasının hacklenmesi ve dönemin valisine kurumun internet sayfasında protesto notu paylaşılması.
11 Mayıs 2013	Hatay Valiliği	Kurumun internet sayfasının çökertilmesi.
26 Mayıs 2013	Avrupa Birliği Bakanı	Dönemin Avrupa Birliği Bakanı’nın maillerinin yayınlanması.
31 Mayıs 2013	Gaziantep Büyükşehir Belediyesi	Kurumun web sayfasının çökertilmesi.
28 Haziran 2013	İstanbul İl Özel İdaresi	Kurumun web sayfasının hacklenmesi ve kurumun kullanıcı bilgilerinin ifşa edilmesi.
02 Temmuz 2013	Sivas İl Özel İdaresi	Kurumun internet sayfasının hacklenmesi ve erişimin tamamen kapatılması.
03 Temmuz 2013	Diyanet İşleri Başkanlığı	Kurumun internet sayfasının hacklenmesi.
14 Ağustos 2013	Adana Büyükşehir Belediyesi Su ve Kanalizasyon İdaresi	Kurumun internet sayfasının hacklenmesi.
14 Ekim 2013	Türkiye Kamu İşletmeleri Birliği	Kurumun internet sayfasının hacklenmesi.
10 Ocak 2014	Türkiye Büyük Millet Meclisi (TBMM)	TBMM’ne ait web sitesinin hacklenmesi.
19 Ağustos 2016	Çanakkale Belediyesi (Hürriyet, 2016)	Kurumun SMS sisteminin hacklenmesi.
04 Ekim 2016	Radio Televizyon Üst Kurulu (RTÜK) (T24, 2016)	Kurumun internet sayfasının hacklenmesi.
25 Mart 2018	Demirören Grubu (T24, 2016)	Kuruma bağlı kuruluşların internet sayfalarının hacklenmesi.
19 Nisan 2018	TRT Çocuk (Cybermag, 2018)	Kurumun internet sayfasının hacklenmesi.

Türkiye’deki kurumları hedef alan, dünya çapında faaliyet gösteren bir diğer grup Anonymous, genellikle gelişen siyasi olaylar neticesinde devlet teşkilatlarına saldırarak protesto eden bir hacker grubudur. İlk zamanları eğlence odaklı bir çevrimiçi topluluk olarak kabul edilen grup, 2008 yılından itibaren, uluslararası internet saldırıları ve protestolar ile anılır hale gelmiştir. Grubun, doğrudan Türkiye’yi hedef alan saldırılarından bazıları Tablo-2’de sunulmuştur.

Tablo-2 Anonymus hacker grubu tarafından kurumlarımıza yapılan saldırılar

Tarih	Kurum	Etkileri
Şubat 2012	BTK (Milliyet, 2012)	Kişisel veriler ve kurumlara ait veriler gibi pek çok veri yayınlanmıştır.
3 Mayıs 2012	TTNET, TÜBİTAK (T24, 2012)	Kurumların internet siteleri devre dışı bırakılmıştır.
25 Ağustos 2012	THY (Radikal, 2012)	Kurumun internet sitesi devre dışı bırakılmış online işlemlerin yapılamaması nedeniyle maddi zarar oluşmuştur.
10 Ekim 2012	THY (Sözcü, 2012)	THY'nin sistemine sızılarak yolcularla ilgili bazı bilgiler ifşa edilmiştir.
12 Haziran 2013	RTÜK (Cumhuriyet, 2013)	Kurumun web sitesi hacklenmiştir.
23 Aralık 2015	#OpTurkey (BBC, 2015)	".tr" uzantılı siteler hedef alınmıştır.
18 Mayıs 2016	Sağlık Bakanlığı (Sözcü, 2016)	Sağlık Bakanlığı'na bağlı 33 devlet hastanesine saldırı düzenlenmiş hasta bilgileri sistemden silinmiştir.

IBM X-Force firması tarafından yayınlanan verilere göre, 2015 yılından itibaren hacktivist saldırıların önemli ölçüde azaldığı, gerçekleşen saldırıların en yoğun olduğu yılda 35 olarak bilinen sayının, 2018 yılında sadece ikiye düştüğü, 2019 yılının ilk birkaç ayı boyunca da bu sayının sıfır olduğu belirtilmiştir. Araştırmacılar, bunun en büyük sebeplerinin, Anonymous'un dağılması ve kanun güçlerinin mücadelesi olduğunu ifade etmişlerdir. Yine IBM'in yayınladığı verilere göre 2011 yılından itibaren ABD, Birleşik Krallık ve Türkiye'de en az 62 tutuklanmanın gerçekleştiği fakat gerçek sayının daha fazla olabileceği bildirilmiştir (Chip Online, 2019). Bu gibi hacktivist grupların saldırıları dışında ülkemiz ve kurumları birçok saldırının hedefi olmuşlardır. Bunun gibi birçok grubun saldırısına maruz kalan Türkiye terör örgütlerinin, arkasında başka devletlerin olduğu saldırılara da maruz kalmaktadır.

20 Ocak 2018'de Türkiye'nin başlatmış olduğu Zeytin Dalı Harekâtı süresince terör örgütleri ve sempatanları uluslararası kamuoyunda algıyı değiştirmek amacıyla "#OpTurkey" başlığı altında, kamu kurum ve kuruluşlarının taşra teşkilatlarına sistematik siber saldırılar düzenlemişlerdir (ANADOLU AJANSI, 2018.a). Türk Silahlı Kuvvetleri ve ülkemiz yıpratılmaya çalışılmıştır.

McAfee yazılım şirketi yayınladığı raporda, Kuzey Koreli olduğu bilinen Hidden Cobra grubu tarafından 02-03 Mart 2018 tarihleri arasında Türk kamu bankalarına yönelik saldırı düzenlendiğini, saldırı sırasında maddi kayıp oluşmadığını ancak saldırıların önümüzdeki dönemlerde planlanan geniş çaplı saldırılar için ön hazırlık olabileceğini belirtmiştir. Aynı zamanda arkasında İranlı bilgisayar korsanlarının olduğu tahmin edilen 2018 yılının Ocak ile Mart ayları arasında başta Türkiye, Pakistan ve Tacikistan olmak üzere birçok ülkenin önemli sanayi tesislerini hedef alan ciddi bir saldırı tespit edilmiştir (STM, t.y.).

24 Haziran 2018'de ülkemiz genelinde yapılan seçimlerde kamu kurumlarımızın web sitelerine ve resmi haber ajanslarına yönelik hizmet dışı bırakma ve manipülasyon gibi amaçlar taşıyan saldırıların gerçekleştiği ve bu saldırıların farklı ülkelerden yapılan saldırılar olduğu belirtilmiştir. Buna karşılık alınan önlemler çerçevesinde 100 kişiye yakın USOM personeli ve diğer kurumlardan toplam 2397 kişinin siber tehditlere karşı seçim boyunca faaliyet gösterdiği belirtilerek sonuçlara yönelik bilgilendirme ve haber yayını engelleme maksadıyla 90 milyonun üzerinde siber saldırıda bulunduğu bildirilmiştir (ANADOLU AJANSI, 2018.b).

ALINABİLECEK ÖNLEMLER

Teknolojideki gelişmeler, siber uzaya dahil olan kullanıcı sayısı ve araç sayısındaki artış, siber saldırılardan kaynaklı zararların maliyetlerindeki yükseliş gibi sebepler, siber güvenliğe yönelik önlem alınmasını her geçen gün daha önemli ve gerekli hale getirmektedir. Siber tehditler ve saldırıların da her geçen gün gelişmesi ve yenilenmesi sebebiyle siber güvenliğe yönelik alınacak önlemlerin sürekliliği bir zorunluluk haline gelmektedir.

Hukuk, teknoloji, organizasyon, kapasite geliştirme ve işbirliği boyutlarındaki 25 göstergeye (indicator) göre ülkelerin taahhüt ettiği siber güvenlik seviyelerini izleyen ve birbirleriyle karşılaştıran, ülkelerin siber güvenlik alanındaki iyileştirme alanlarını tespit etmelerine yardımcı olan böylece dünya genelindeki siber güvenlik seviyesinin yükselmesini amaçlayan Küresel Siber Güvenlik Endeksi (Global Cybersecurity Index- GCI)’ne göre Türkiye 2018 yılında ITU’ya üye 193 ülkeden çalışmaya katılan 155’i arasında 22’nci sırada bulunmaktadır. GCI’nın 2018 yılı raporunda; siber suç mevzuatının uygulanması, ulusal siber güvenlik stratejileri, bilgisayar olaylarına müdahale ekipleri, stratejileri yayma konusunda farkındalık ve kapasite ile siber güvenlik alanındaki yetenekler ve programlar açısından birçok ülke arasında gözle görülür farklılıklar olduğu belirtilmektedir (International Telecommunication Union, 2019).

Türkiye’de son yıllarda siber güvenliğin sağlanmasına yönelik önemli çalışmalar yapılmaktadır. Kamu kurum ve kuruluşları önderliğinde hem sivil toplum örgütleri hem de özel sektör iş birliği ile siber güvenlik stratejileri geliştirilmektedir. Ancak Türkiye’ye gerçekleştirilen saldırılar göz önüne alındığında ortalamanın üzerinde bir oranda saldırıya uğraması ve en fazla siber saldırıya maruz kalan ülkelerden olması, yapılanların alınan önlemler bakımından olmasa da siber caydırıcılık bakımından yeterli olmadığını göstermektedir. Türkiye’nin jeopolitik önemi göz önüne alındığında bölgesinde güçlü bir ülke olmak zorundadır. Bu bakımdan, artık milli güç unsurlarından “Bilimsel ve Teknolojik Güç” içerisinde kabul edilen “Siber Güç (siber savunma, taarruz ve caydırıcılık gücü)”ünün (Şenol, 2017: 16) de belirli/yeterli bir seviyenin üzerinde olması bir gerekliliktir. Her ne kadar dünyadaki gelişmiş ülkelerin bilgi güvenliği ve siber güvenliğin sağlanmasına yönelik çalışmalarının geçmişi daha eskilere dayansa ve yatırımlarının oranı daha fazla olsa da örneğin Ukrayna’nın GCI 2018 raporunda dördüncü sırada olması, Türkiye’nin de ilk sıralardaki ülkelerle arasındaki açığı kapatarak siber güvenlik yetkinliğini artırabileceğini gösteren önemli motivasyonlardan birisidir. Yapılan analizlerden çıkarımlar ile kurumlarda ve hayati öneme sahip kritik tesislerde güvenliğin sağlanması için alınabilecek önlemler aşağıda sıralanmıştır:

- Siber güvenlik ile ilgili stratejiler ve politikalar belirlenmelidir.
- Bireylerde farkındalık oluşturacak faaliyetler yürütülmelidir.
- Kurumlar arası iş birliği ve koordinasyonun sağlanması amacıyla kurum içinde birimler oluşturulmalıdır.
- Uluslararası ve ulusal iş birliğinin artırılması maksadıyla tatbikatlar icra edilmelidir
- Siber saldırıların önlenmesi ve siber caydırıcılığın sağlanması amacıyla hukuksal altyapı kuvvetlendirilmelidir.
- Siber saldırıların tespiti ve önlenmesine yönelik teknik altyapı sağlanmalıdır.
- Nitelikli insan gücünün artırılması sağlanmalı bu maksatla lisans ve lisansüstü programlar yürütülmelidir (Önaçan ve Atan, 2016),
- Siber güvenlik yatırımları artırılmalıdır.
- Siber saldırı sonucu oluşabilecek etkiyi azaltmak için planlar yapılmalıdır.
- Sistemlerde kullanılan yazılımlar düzenli olarak güncellenmelidir.
- Yerli ve milli yazılım geliştirilmeli, üretim sektörü desteklenmelidir

- Sistemlerdeki açıkların ve zafiyetlerin tespitinde, hem siber saldırı hem de siber savunma için yapay zekadan yararlanılmalıdır.

SONUÇ

Araştırma sonucunda elde edilen bilgiler doğrultusunda Türkiye'nin tüm Avrupa hatta dünya ülkelerine kıyasla daha çok siber saldırıya maruz kaldığı anlaşılmaktadır. Saldırı çeşitleri incelendiğinde daha çok finans sektörünün hedef alındığı tespit edilmiştir. Ayrıca ülkemizin bulunduğu coğrafyadaki siyasi istikrarsızlıklar, artan çatışmalar ve bunların küresel etkileri göz önüne alındığında saldırıların kişisel menfaatler dışında ülkemiz üzerinde siyasi baskı aracı olarak kullanıldığı da görülmektedir. Bunların yanı sıra ülkemiz sadece dış kaynaklı saldırılara maruz kalmamakta zaman zaman ülkemiz içerisinde de değişik hacker grupları tarafından çeşitli kurumlara saldırılar düzenlenmektedir. Bu gelişmeler neticesinde ülkemizde siber güvenlik amacıyla kurumlar oluşturulmuş, yasal düzenlemeler yapılmış ve birtakım önlemler alınmıştır. Siber güvenlik alanında alınan önlemler incelendiğinde özellikle son 5 yılda büyük gelişmeler kaydedildiği görülmektedir. Ulusal Siber Güvenlik Eylem Planları, Yasal Çalışmalar, Siber Olaylara Müdahale amacıyla oluşturulan kurumlar, Siber Güvenlik Tatbikatları, Toplumsal farkındalık çalışmaları, çalıştaylar, TSK bünyesinde yapılan faaliyetler bu gelişmelerdendir. Ancak bu gelişmelere rağmen, ülkemize yapılan siber saldırıların diğer ülkelere kıyasla daha fazla olması, alınan tedbirlerin engelleyici ve caydırıcı nitelikte olmadığını göstermektedir. Firmaların, kamu kurumlarının, hükümet yetkililerinin ve bireylerin siber alanda hedef olması nedeniyle siber caydırıcılığın sağlanması önem arz etmektedir. Bu alana daha fazla yatırım yapılması gerekliliği ortaya çıkmaktadır. Bu bağlamda olması muhtemel siber saldırılarda caydırıcılığı sağlamak amacıyla; saldırılar oluşmadan önce etkili önlemler alınmalıdır. Her geçen gün değişik metotlarla geliştirilen siber saldırılara karşı toplumsal bilincin oluşturulması, kurumlar arası iş birliğinin artırılması ve suçluların yakalanması amacıyla uluslararası iş birliğinin sağlanması, ulusal menfaatlerimiz açısından vazgeçilmezdir. Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile bir bütün olarak ele alan yaklaşım benimsenmelidir. Tüm bunlarla birlikte bilişim sistemlerinde, iletişim teknolojilerinde milli ve yerli çözümlere sahip olunmalıdır. Siber saldırıların meydana getireceği bir aksaklık sonucunda oluşacak zararın, bu alanda yapılacak yatırımlardan çok daha fazlasına mal olabileceği göz önüne alınarak siber savunmaya daha fazla yatırım yapılması gerekmektedir.

KAYNAKÇA

- AHaber. (2015). *Siber Saldırı Değil Savaş*, Yayımlanma Tarihi: 28.12.2015, 05.12.2019 tarihinde <https://www.ahaber.com.tr/gundem/2015/12/28/siber-saldiri-degil-savas> adresinden erişildi.
- Akamai. (2017). State of the Internet/ Security, Q2 2017 Report, 4 (2), 05.12.2019 tarihinde <https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf> adresinden erişildi.
- Alkan, M. (2012). Siber Güvenlik ve Siber Savaşlar, Siber Güvenlik Siber Savaşlar TBMM Internet Komisyonu, Mayıs'dan aktaran ASLAY, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi, *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1 (1), 24-28.
- Altınkaynak, M. (2017). *Uygulamalı Siber Güvenlik ve Hacking*, 5. Baskı, Abaküs Yayınları.
- Altun, A (2017). ABD-ÇİN Rekabeti Bağlamında Siber Savaş, *International Journal of Academic Value Studies*, 3 (9), 24-34.
- Anadolu Ajansı. (2018.a). Zeytin Dalı Harekatı'nda siber saldırılar arttı, Yayımlanma Tarihi: 14.04.2018, 05.12.2019 tarihinde <https://www.aa.com.tr/tr/turkiye/zeytin-dali-harekatinda-siber-saldirilar->

- artti/1117914 adresinden erişildi.
- Anadolu Ajansı. (2018.b). Siber saldırılar AA'yı engelleyemedi, Yayınlanma Tarihi: 26.06.2018, 24.05.2019 tarihinde <https://www.aa.com.tr/tr/secim-2018/siber-saldirilar-aayi-engelleyemedi/1187982> adresinden erişildi.
- BBC. (2015). Türkiye’ye siber saldırının 10 günü: Ne oldu?. Yayın Tarihi: 24.12.2015, 02.01.2019 tarihinde https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan adresinden erişildi.
- Biçakçı, S., Doruk, E., & Çelikpala, M. (2016). Türkiye’de Siber Güvenlik ve Nükleer Enerji. 10.06.2019 tarihinde http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf adresinden erişildi.
- Biçakçı, S., Ergun, D. & Çelikpala, M. (2015). Türkiye’de Siber Güvenlik 14.05.2019 tarihinde http://edam.org.tr/wp-content/uploads/2015/12/EDAM_TR_Siber_Guv_1.pdf adresinden erişildi.
- BTK. (2016). Türkiye’de Bilişim Hukuku. 29.04.2019 tarihinde <http://internet.btk.gov.tr/turkiye-de-bilisim-hukuku-detay-70.html> adresinden erişildi.
- BTK. (2017). Mevzuat-Bilgi Teknolojileri ve İletişim Kurumu. 23.08.2019 tarihinde <https://www.btk.gov.tr/siber-guvenlik-mevzuat> adresinden erişildi.
- Chiponline. (2018). Türkiye için iyi haber! Fidyе Saldırıları Azaldı, Yayınlanma Tarihi: 08.07.2018, 05.12.2019 tarihinde https://www.chip.com.tr/haber/turkiye-icin-iyi-haber-fidye-saldirilari-azaldi_76867.html adresinden erişildi.
- Chiponline, (2019). Anonymous'un Ardından İşler Değişti, 24.05.2019, Yayınlanma Tarihi: 05.12.2019 tarihinde https://www.chip.com.tr/haber/anonymousun-ardindan-isler-degisti_82374.html adresinden erişildi.
- Cnntrk. (2017). Türkiye de dahil 74 ülkeye siber saldırı. Yayınlanma Tarihi: 12.05.2017, 19.05.2019 tarihinde <https://www.cnntrk.com/turkiye/turkiye-de-dahil-74-ulkeye-siber-saldiri> adresinden erişildi.
- Cumhuriyet. (2016). Hackerler Türkiye’de en çok ‘5 yöntemle saldırıyor, Yayınlanma Tarihi: 02.03.2016, 19.05.2019 tarihinde http://www.cumhuriyet.com.tr/haber/turkiye/490665/Hackerler_Turkiye_de_en_cok_5_yontemle_saldiriyor.html adresinden erişildi.
- Cumhuriyet (2019). Türkiye, kimlik avı saldırısında ilk sırada, Yayınlanma Tarihi: 05.05.2019, 22.05.2019 tarihinde http://www.cumhuriyet.com.tr/haber/turkiye/1379237/Turkiye_kimlik_avi_saldirisinda_ilk_sirada.html adresinden erişildi.
- Cumhuriyet. (2013). Yayın Tarihi: 12.06.2013, 24.12.2015 tarihinde http://www.cumhuriyet.com.tr/haber/diger/427378/Anonymous_RTUK_u_Hackledi.html adresinden erişildi.
- Cybermag. (2018). TRT Çocuk Hacklendi ! - CyberMag. Yayın Tarihi: 19.04.2018, 02.01.2019 tarihinde <https://www.cybermagonline.com/trt-cocuk-hacklendi> adresinden erişildi.
- Çiftçi, H. (2013). Her Yönüyle Siber Savaş, 2’nci Baskı, Ankara: TUBİTAK.
- Daricili, A.B (2017). Demokrat Parti Hack Skandalı Bağlamında ABD ve RF’nin Siber Güvenlik Stratejilerinin Analizi. Ulusa: Uluslararası Çalışmalar Dergisi, Özel Sayı, 1-24.
- Daricili, A.B. (2019). Türkiye’nin Siber Güvenlik Politikalarının Analizi; Türkiye’nin Potansiyel Siber Güvenlik Stratejisi, TESAM Akademi Dergisi, Temmuz, 6 (2), 11-33.
- Demirel, F. (2016). Bugün açıklanan Ulusal e-Devlet ve Siber Güvenlik Strateji ve Eylem Planı’nda hangi hedefler var?, 05.12.2019 tarihinde <https://webrazzi.com/2016/09/09/bugun-aciklanan-ulusal-e-devlet-ve-siber-guvenlik-strateji-ve-eylem-planlarinda-hangi-hedefler-var> adresinden erişildi.

- EGM. (t.y.). Hakkımızda. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, 10.06.2019 tarihinde <https://www.egm.gov.tr/siber/hakkimizda2> adresinden erişildi.
- Eset. (2017). Released Android malware source code used to run a banking botnet, Yayınlanma Tarihi: 23.02.2017, 22.05.2019 tarihinde <https://blog.eset.ie/2017/02/23/released-android-malware-source-code-used-to-run-a-banking-botnet/> adresinden erişildi.
- Fas.Org. (1997). Russian National Security Blueprint 13.05.2019 tarihinde <https://fas.org/nuke/guide/russia/doctrine/blueprint.html> adresinden erişildi.
- Gürkaynak, M., & İren, A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Dergisi, 16 (2), 263-279.
- Habertürk. (2019). Fidyе saldırılarında Türkiye, Avrupa’da ilk sırada yer aldı!, Yayınlanma Tarihi: 19.03.2019, 17.05.2019 tarihinde <https://www.haberturk.com/turkiye-ye-yonelik-fidye-yazilimi-saldirisi-artiyor-2408206-teknoloji> adresinden erişildi.
- Hekim, H. (2015). Oltalama (Phishing) Saldırıları, 19.05.2019 tarihinde https://www.academia.edu/35136881/Oltalama_Phishing_Saldirilari adresinden erişildi.
- Hürriyet. (2016). Türkiye’de en çok karşılaşılan 5 siber saldırı çeşidi. Yayınlanma Tarihi: 10.04.2016, 05.12.2019 tarihinde <http://www.hurriyet.com.tr/egitim/turkiyede-en-cok-karsilasilan-5-siber-saldiri-cesidi-40085097> adresinden erişildi.
- Hürriyet. (2016). Çanakkale Belediyesi'nin SMS sistemi hacklendi. Yayın Tarihi:19.08.2016, 02.01.2019 tarihinde <http://www.hurriyet.com.tr/canakkale-belediyesinin-sms-sistemi-hacklendi-40202015> adresinden erişildi.
- Hürriyet. (2018). DDoS saldırıları son çeyrekte 2 kat arttı, Yayınlanma Tarihi: 29.03.2019, 05.12.2019 tarihinde <http://www.hurriyet.com.tr/teknoloji/ddos-saldirilari-son-ceyrek-2-kat-artti-40787977> adresinden erişildi.
- Hürriyet. (2019). Eğitim sektörü fidye yazılımı saldırılarıyla boğuşuyor. Yayınlanma Tarihi: 18.04.2019, 05.12.2019 tarihinde <http://www.hurriyet.com.tr/teknoloji/egitim-sektoru-fidye-yazilimi-saldirilariyla-bogusuyor-41186437> adresinden erişildi.
- International Telecommunication Union (ITU), (2019). Global Cybersecurity Index 2018, ITU Publications.
- KasperskyLab. (2016). Fidyе yazılımı nedir? Yayınlanma Tarihi: 15.12.2016, 05.12.2019 tarihinde <https://www.kaspersky.com.tr/blog/ransomware-for-dummies/2713/> adresinden erişildi.
- KasperskyLab. (2017). Türkiye’de fidye yazılımları şirketleri hedef alıyor: 2017’de fidye yazılımlarının hedef aldığı kullanıcıların %43’ünü şirketler oluşturdu. Yayınlanma Tarihi: 12.12.2017, 19.05.2019 tarihinde https://www.kaspersky.com.tr/about/press-releases/2017_turkiye-de-fidye-yazilimleri-sirketlerihedef-aliyor-2017-de-fidye-yazilimlarinin-hedef-aldigi-kullanicilarin-43-unu-sirketler-olusturdu adresinden erişildi.
- KasperskyLab. (2018). Middle East Focused Threat Actor Muddy Water Extend Attacks Towards Government Targets in Asia, Europe and Africa, Yayınlanma Tarihi: 10.10.2018, 19.05.2019 tarihinde https://www.kaspersky.com/about/press-releases/2018_muddy-water-final adresinden erişildi.
- Kuru, E., Onaçan, M.B.K. & Önel, T. (2019). The Effects of Internet of Things (IoT) in Cyber War: A Conceptual Approach, 1st International Symposium on Implementations of Digital Industry and Management of Digital Transformation 2019, 25-26 Haziran 2019, Konya-Türkiye, 319-325.
- Milliyet. (2012). THY 6 saatte 400 bin lira zarar etti, Yayınlanma Tarihi: 26.08.2012, 05.12.2019 tarihinde <http://www.milliyet.com.tr/thy-6-saatte-400-bin-lira-zarar-etti-ekonomi-1586632/> adresinden erişildi.
- Milliyet. (2012). Anonymous’?BTK’nın sırlarını çaldı. Yayın Tarihi: 15.02.2012, 02.01.2019 tarihinde

- <http://www.milliyet.com.tr/gundem/anonymous-btk-nin-sirlarini-caldi-1502259> adresinden erişildi.
- Öğün, M.N. & Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler, *Güvenlik Stratejileri*, 9 (18), 145-181.
- Önaçan, M.B.K. & Atan, H. (2016). Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği, *Trakya University Journal of Engineering Sciences*, 17 (1), 13-21.
- Önaçan, M.B.K. & Yıldırım, C.C. (2016). Üniversite Öğrencilerinin Siber Güvenlik Farkındalığını Artırmaya Yönelik Bir Yol Haritası, *International Conference on Quality in Higher Education*, 24-25 Kasım 2016, Sakarya-Türkiye, 948-955.
- Radikal. (2012). Yayın Tarihi: 26.08.2012, 02.01.2019 tarihinde <http://www.radikal.com.tr/ekonomi/grev-yapan-isciler-icin-thynin-fisini-cektiler-1098232/> adresinden erişildi.
- Resmi Gazete, (2007) İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayılar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. 21.04.2019 tarihinde <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf> adresinden erişildi.
- Resmi Gazete, (2011). Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, 01.12.2019 tarihinde <https://www.resmigazete.gov.tr/eskiler/2011/11/20111101M1-1.htm> adresinden erişildi.
- Sherstobitoff, R. (2018). Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant McAfee Blogs, Yayınlanma Tarihi: 08.03.2018, 19.05.2019 tarihinde <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/> adresinden erişildi.
- Sonicwall. (2018). 2018 Sonicwall Siber Tehdit Raporu, 05.12.2019 tarihinde http://www.m2s.com.tr/bulten/2018_Sonicwall_siber_tehdit_raporu-TR.pdf adresinden erişildi.
- STM. (2016). Dönemi Siber Tehdit Durum Raporu Temmuz-Eylül 2016 yayınlandı, 18.05.2019 tarihinde <https://www.stm.com.tr/tr/haberler/duyurular/siber-tehdit-durum-raporu-temmuz-eylul-2016-yayinlandi> adresinden erişildi.
- STM, (t.y.). 2018 Ocak-Mart Dönemi Siber Tehdit Durum Raporu, 21.09.2019 tarihinde <https://www.stm.com.tr/documents/file/Pdf/siber-tehdit-durum-raporu-ocak-mart-2018.pdf> adresinden erişildi.
- Sözcü. (2012). THY’ye 2. hacker şoku. Yayın Tarihi: 10.10.2012, 05.12.2019 tarihinde <https://www.sozcu.com.tr/2012/gundem/thyye-2-hacker-soku-76033/> adresinden erişildi.
- Sözcü. (2016). 33 hastaneye siber saldırı. Yayın Tarihi: 18.05.2016, 02.01.2019 tarihinde <https://www.sozcu.com.tr/2016/gundem/33-hastaneye-siber-saldiri-1235714/> adresinden erişildi.
- Şenol, M. (2017) Türkiye’de Siber Saldırlara Karşı Caydırıcılık, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 3 (2), 1-9.
- Takvim. (2019). Kredi kartı kullananlar dikkat! Yılda 100 bin kişi bu yöntemlerle dolandırılıyor. Yayınlanma Tarihi: 24.04.2019, 05.12.2019 tarihinde <https://www.takvim.com.tr/ekonomi/2019/04/24/kredi-karti-kullananlar-dikkat-yilda-100-bin-kisi-bu-yontemlerle-dolandiriliyor?paging=3> adresinden erişildi.
- Taşçi, U. & Can, A. (2015) Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014, *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 25 (2), 233-235.
- Sputniknews, (2019). Türkiye, banka kartı sayısında Avrupa’da birinci, Yayınlanma Tarihi: 26.02.2019, 02.12.2019 tarihinde <https://tr.sputniknews.com/turkiye/201902261037890762-turkiye-banka-karti-sayisinda-avrupa-birincisi/> adresinden erişildi.
- Turak, Y. (2014). RedHack Özelinde Siber Olaylar ve Siber Suçlar. 21.09.2019 tarihinde <http://www.yigitturak.com/wp-content/uploads/RedHackIncelemesi.pdf> adresinden erişildi.

- TÜBİTAK. (2019). Tarihçe Siber Güvenlik Enstitüsü 16.05.2019 tarihinde <https://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce> adresinden erişildi.
- T24. (2012). Anonymous'tan RedHack'e 'süt' desteği. Yayın Tarihi: 03 Mayıs 2012, 25.09.2019 tarihinde <https://t24.com.tr/haber/redhack-ve-anonymous-dayanismasi,203081> adresinden erişildi.
- T24. (2016). RedHack RTÜK'ün internet sitesini hackledi. Yayın Tarihi: 04.10.2016, 02.01.2019 tarihinde <https://t24.com.tr/haber/redhack-rtukun-internet-sitesini-hackledi,363173> adresinden erişildi.
- T24. (2018). Redhack, Erdoğan Demirören'e ait siteleri hackledi: Duyduk ki Doğan Medya'yı almış... Yayın Tarihi: 25 Mart 2018, 25.09.2019 tarihinde <https://t24.com.tr/haber/redhack-erdogan-demirorene-ait-siteleri-hackledi-duyduk-ki-dogan-medyayi-almis,589827> adresinden erişildi.
- USOM (2014). Siber Güvenliğe İlişkin Temel Bilgiler. Ulusal Siber Olaylara Müdahale Merkezi (USOM-TRCERT), Temmuz. 05.12.2019 tarihinde <http://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2014-Siber%20G%C3%BCvenli%C4%9Fe%20%C4%B0li%C5%9Fkin%20Temel%20Bilgiler.pdf> adresinden erişildi.
- USOM. (t.y.). USOM Hakkında. Ulusal Siber Olaylara Müdahale Merkezi. 10.06.2019 tarihinde <https://www.usom.gov.tr/> adresinden erişildi.
- UDHB. (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 05.12.2019 tarihinde <https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf> adresinden erişildi.
- UDHB, (t.y.). 2016-2019 Ulusal Siber Güvenlik Stratejisi, 05.12.2019 tarihinde <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf> adresinden erişildi.
- Ünver, M., Canbay, C., & Mirzaoglu, A. (2011). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, 1. Basım, ISBN: 978-9944-0189-6-8, 22-24.
- Yegen, C. (2014). Dijital Aktivizmin Bir Türü Olarak Hacktivizm ve "Redhack". E-Journal of Intermedia, 1 (1), 118-132.
- Yenişafak, (2017). Siber saldırıların maliyeti yılda 500 milyar dolar, Yayın Tarihi: 16 Mart 2017, 25.09.2019 tarihinde <https://www.yenisafak.com/teknoloji/siber-saldirilarin-maliyeti-yilda-500-milyar-dolar-2629430> adresinden erişildi.
- Yılmaz, A. (2015). Türkiye'deki Dolandırıcılık Tipolojileri: Dolandırıcılık Olaylarının Kategorik Tasnifi ve Yapılış Şekilleri, Sosyolojik Araştırmalar Dergisi, Yayımlanma Tarihi: 13.12.2015, 05.12.2019 tarihinde <http://www.sdergi.hacettepe.edu.tr/?page=makaleler> adresinden erişildi.