Ortaöğretim Kurumlarında Uygulanan Siber Güvenlik Farkındalık Eğitiminin Öğrenciler Üzerindeki Etkisi

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Hüsnü TAVLAŞ

tarafından

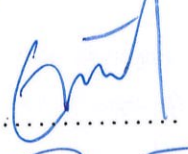
Fen Bilimleri Enstitüsü'ne
sunulmuştur.

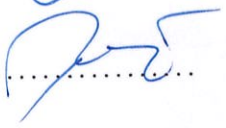
İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Prof. Dr. Selim Zaim ..... 
(Tez Danışmanı)

Prof. Dr. Ensar Gül ..... 

Prof. Dr. Nizamettin Bayyurt ..... 

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 17/07/2019

MÜHÜR/İMZA: 

Yazarlık Beyanı

Ben, Hüsnü TAVLAŞ, başlığı, 'Ortaöğretim Kurumlarında Uygulanan Siber Güvenlik Farkındalık Eğitiminin Öğrenciler Üzerindeki Etkisi' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: _____

Tarih: 17 /07 /2019

Ortaöğretim Kurumlarında Uygulanan Siber Güvenlik Farkındalık Eğitiminin Öğrenciler Üzerindeki Etkisi

Hüsnü Tavlaş

Öz

Bilgisayarlar yaşamın her yerindedir ve tüm veriler bilgisayarlar aracılığı ile paylaşılmakta ve saklanmaktadır. Devlet kurumlarından işletmelere ve kişilere kadar herkesin bilgi güvenliği konusunda bilinçli olması gerekir. Aksi takdirde, ekonomik sorunlar ortaya çıkabilecek, bilgi hırsızlığı ile kaynak tüketimi artabilecek, dolandırıcılık gibi suçlar çoğalabilecektir. Tüm bunların yanında ülkelerin güvenlikleri de tehlikeye düşebilecektir. Bu nedenle ulusal bir mesele haline gelen siber güvenlik konusunda yarının karar vericileri olarak çocukların eğitilmesi, bireysel risklerin düşmesinde etkili olacaktır. Bireysel risklerin azalması doğru orantılı olarak, ulusal siber risklerin azalmasında da etkili olacaktır. Bu çalışmada özellikle eğitim alanındaki AB, ABD ve Türkiye'nin Siber Güvenlik Stratejileri incelenmiş ve birbirleri ile karşılaştırılmıştır. Bireysel siber risklerin azaltılmasına yönelik yapılan alan araştırmasında da 211 ortaokul 5nci sınıf öğrencisine bilgi güvenliği farkındalık eğitimi verilmiştir. Kişisel güvenliği sağlama ve siber zorbalığa ilişkin duyarlılık ölçekleri kullanılmıştır. Eğitim öncesi ve sonrası yapılan anketlerle aradaki fark ölçülmüştür. Verilen bilgi güvenliği farkındalık eğitiminin ortaokul öğrencilerinin kişisel siber güvenliği sağlama ve siber zorbalığı farkındalıkta pozitif etkisi olduğu görülmüştür.

Anahtar Sözcükler: İnternet, Siber Güvenlik, AB, ABD, Türkiye

The Impact of Cyber Security Awareness Training on Students in Secondary Education Institutions

Hüsnü Tavlaş

Abstract

Computers are in every sphere of life and all data is shared and stored through computers. Everyone, from government institutions to enterprises and individuals, must be aware of cybersecurity. Otherwise, economic problems may arise, information theft and resource consumption may increase, and crimes such as fraud may be multiplied. In addition to all these, the security of the countries may be compromised. Therefore, the education of children as tomorrow's decision makers on cybersecurity, which has become a national issue, will be effective in reducing individual risks. The reduction of individual risks will also be directly proportional to the reduction of national cybercrime risks. In this study, cybersecurity strategies of the EU, USA and Turkey, especially in the field of education, have been examined and compared with each other. In the field research aimed at reducing individual cyber risks, 211 Middle School 5th grade students were given cybersecurity awareness training. Sensitivity scales for personal safety and cyber-bullying were used. The difference was measured by questionnaires conducted before and after the training. The cybersecurity awareness training given has been shown to have a positive effect on the awareness of cyber-bullying and providing personal cybersecurity for secondary school students.

Keywords: Internet, Cyber Security, AB, USA, Turkey

Teşekkür

Çalışmayı yürüttüğüm süre zarfında bana her an yardım ve desteğini esirgemeyen tez danışmanım Sayın Prof. Dr. Selim Zaim hocama şükranlarımı sunuyorum. Ayrıca, tez çalışmam sürecinde destek olan Bilgi Güvenliği Yüksek Lisans Programı Koordinatörü Sayın Prof. Dr. Ensar Gül hocama teşekkür ederim.

Yüksek lisans için beni cesaretlendiren ve destek olan sevgili annem Aysel Tavlaş'a ve çalışma süreci boyunca beni yalnız bırakmayan ve desteklerini her zaman hissettiğim sevgili kızım Eylül Elif Tavlaş ve sevgili eşim Nihal Tavlaş'a teşekkürü bir borç bilirim.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

AB	**A**vrupa **B**irliği
G2C	**G**overnment to **C**itizen /Devletten Vatandaşa
G2B	**G**overment to **B**usiness/Devletten İş Dünyasına
G2G	**G**overment to **G**overment/Devletten Devlete
USA	**U**nited **S**tates of **A**merica
ABD	**A**merika **B**irleşik **D**evletleri
IoT	**I**nternet **o**f **T**hings
FBI	**F**ederal **B**ureau of **I**nvestigation /Federal Araştırma Bürosu
CIA	**C**entral **I**ntelligence **A**gency/ Merkezi Haber Alma Servisi
DHS	United States **D**epartment of **H**omeland **S**ecurity/ ABD İç Güvenlik Bakanlığı
CYBERCOM	United States Department of Defense/ ABD Siber Komutanlık
NSA	**N**ational **S**ecurity **A**gency/ Ulusal Güvenlik Ajansı
NICIC	**N**ational **C**yber Security and **C**ommunications **I**ntegration **C**enter/ Ulusal Siber Güvenlik ve iletişim Entegrasyon Merkezi
CSS	National Security Servise / Merkezi Güvenlik Servisi
ICI-IPC	**I**nformation and **C**ommunications **I**nfrastructure Interagency Policy Committee / Bilgi ve İletişim Altyapıları Kurumlar Arası Politika Komitesi
DoJ	The **D**epartment **o**f **J**ustice/Adalet Bakanlığı
NICE	**N**ational **I**nitiative for **C**ybersecurity **E**ducation/ Ulusal Siber Güvenlik Eğitim Girişimi
EC3	**E**uropean **C**ybercrime **C**entre/ Avrupa Siber Suç Merkezi
CERT	**C**omputer **E**mergency **R**eadiness **T**eam/ Bilgisayar Acil Müdahale Ekibi
ENISA	European Union Agency For Network and Information Technology

ECSM	**E**uropean **C**yber **S**ecurity **M**onth
OECD	Ekonomik İş Birliği ve Kalkınma Teşkilatı
WPISP	Kuruluşun Bilgi Güvenliği ve Gizlilik Çalışma Grubu
ICCP	Bilgi, Bilgisayar ve Haberleşme Politikaları Komitesi
NATO	Kuzey Atlantik İttifakı
FATİH	**F**ırsatları **A**rttırma ve **T**eknolojiyi **İ**yileştirme **H**areketi
RTÜK	**R**adyo ve **T**elevizyon **Ü**st Kurulu
UDHB	**U**laştırma, **D**enizcilik ve **H**aberleşme **B**akanlığı
TC	**T**ürkiye **C**umhuriyeti
MSB	**M**illî **S**avunma **B**akanlığı
MİT	**M**illî **İ**stihbarat **T**eşkilâtı
BTK	**B**ilgi **T**eknolojileri ve İletişim **K**urumu
MASAK	**M**ali **S**uçları **A**raştırma **K**urulu
TİB	**T**elekomünikasyon **İ**letişim **B**aşkanlığı
EPDK	**E**nerji **P**iyasası **D**üzenleme **K**urumu Başkanlığı
YSK	**Y**üksek **S**eçim **K**urulu Başkanlığı
KİK	**K**amu **İ**hale **K**urumu Başkanlığı
HSYK	**H**âkimler ve **S**avcılar **Y**üksek **K**urulu Başkanlığı
TCMB	**T**ürkiye **C**umhuriyeti **M**erkez **B**ankası Başkanlığı
YÖK	**Y**ükseköğretim **K**urulu Başkanlığı
SPK	**S**ermaye **P**iyasası **K**urulu Başkanlığı

Bölüm 1

Giriş

Günümüzde teknoloji hayatımızın her alanında yer almaktadır. Teknolojinin hızla gelişmesi ve buna oranla yayılması kişilerin, kurumların ve devletlerin internete bağlılığını da arttırmış durumdadır. Günlük hayatımızda interneti kullanarak, alışveriş yapabilmek, bankacılık uygulamaları ile finansal işlemlerimizi ve ödemelerimizi gerçekleştirmek, acıktığımızda yemek siparişi vermek mümkün hale gelmiştir. Navigasyon uygulamaları ile gideceğimiz adrese dahi internet kullanarak ulaşabilmek, akıllı telefon, tablet bilgisayarlar vb. mobil cihazlar kullanarak, zaman ve mekândan bağımsız olarak tüm bu işlemleri kolaylıkla yapabilmek artık oldukça kolaydır.

Ülkemizde 2017 yılı araştırmalarına göre, hanelerin yüzde 80,7'si evinden internete ulaşabiliyorken, yüzde 78,3'ü geniş bant internet erişimine sahiptir [1]. 2017 yılı 3 aylık Türkiye İstatistik Kurumu (TÜİK) araştırmalarına göre internete ulaşan 16 -74 yaş grubundaki kişilerin 83,7'lik yüzdesinin sosyal medya özelliği taşıyan web sitelerinde bir hesaba sahip oldukları, buralarda iletişim kurdukları ve etkileşime girdikleri rapor edilmiştir [2].

İnternet teknolojisi ile hayatımıza giren sosyal medya kavramı, kişiler arasındaki iletişimi güçlendirmekle kalmayıp kurumların da sosyal medyaya dahil olmasıyla kişiler ve kurumlar arasındaki iletişimi de kolaylaştırmış ve artmasına yol açmıştır. Geleneksel medyadan farklı olarak, sosyal medya kişi ve kurumlar arasında çift taraflı etkileşimin de başlangıcı olmuştur.

Dijital pazarlama ajansı We Are Social ve Hootsuite iş birliği ile hazırlanan "Digital in 2018 Q2 Global Overview" Raporu'na göre Dünya'da 4.021 milyar internet hesabı bulunmaktadır. Sosyal ağ kullanımında, Facebook 2.167 milyar, Youtube 1,5 milyar ve

Whatsapp 1,3 milyar kullanıcı sayıları ile ilk üç sırada yer almaktadır. Yine aynı araştırmaya göre Facebook Türkiye'de aktif 51 milyon kullanıcıya sahiptir [3]. Sosyal medyada oluşan güvenlik açıklarının en temel sebeplerinden biri, mahremiyetin korunamaması ve oluşturulan hesap ve profiller üzerinden yüklenen ve paylaşılan video, fotoğraf, metin paylaşımları ile kişisel bilgileri kişinin kendi rızası ile paylaşarak kendilerini hedef haline getirmeleridir [4].

17 Mart 2018 tarihinde Newyork Times ve The Observer of London Gazeteleri tarafından yapılan bir haberde, Facebook kullanıcılarına ait kişisel verilerin Cambridge Analytica isimli bir şirket tarafından toplandığı ve saklandığı; bu verileri de seçim ve propaganda amaçlı paylaştığı belirtilmektedir. Bu noktada, şirketin uluslararası kişisel verilerin korunmasına yönelik düzenlenmiş olan yasalara da aykırı davrandığını söylemek gerekmektedir. Facebook, milyonlarca kişiye ait veriyi Amerika Birleşik Devletleri'nde (ABD) 2016 yılında gerçekleşen başkanlık seçimlerini manipüle etmekle suçlanmıştır. Büyük yankı uyandıran bu haber üzerine Facebook 87 milyon kişiye ait verinin Cambridge Analytica adlı şirketle uygunsuz olarak paylaşılmış olabileceğini açıklamıştır. Konuya ilişkin ABD Federal Ticaret Komisyonu tarafından soruşturma başlatılmıştır [5]. 2013 yılında yayımlanan Cisco Güvenlik Raporu'na göre güvenlik tehdidinin en çok sosyal medyada söz konusu olduğu belirtilmiştir [6]. Sosyal medya kullanımının artışıyla riskler de doğru orantılı bir şekilde artmaktadır.

İnternetin kullanımının artması ve hemen her yaş aralığında yaygınlaşmasıyla kurumların verdiği hizmetlerin internet platformuna taşınması da bir zorunluluk haline gelmiştir. Bu noktada internet üzerinden ürün ve hizmetlerin satışa çıkarıldığı e-ticaret kavramı ortaya çıkmıştır. Mağazacılık, ulaştırma, medya, sigorta, eğitim ve sağlık gibi çok sayıda sektör internet üzerinden Business to Consumer (B2C) -işletmeden müşteriye- ve Business to Business (B2B) -işletmeden işletmeye- ticari faaliyetleri gerçekleştirmeye başlamış, bu durum ticari faaliyetlerin sürdürülebilmesi için bir zorunluluk haline gelmiştir. İnternet kullanarak müşterilere ve iş ortaklarına ulaşmak, işletmelerin maliyetlerini düşürmekte ve rekabet avantajını beraberinde getirmektedir.

Bilgi toplumuna geçiş sürecinde devletler de teknolojik gelişmeler, uluslararası rekabet ve toplumsal talepler karşısında kayıtsız kalmayarak vatandaşlarına sunduğu hizmetleri internet platformu üzerine taşımış e-devlet kavramı altında çok sayıda kamu hizmetini vatandaşlarının hizmetine sunmuştur [7]. Goverment to Citizen -Devlet – vatandaş- (G2C),

Goverment 2 Business (G2B) -Devlet – iş dünyası-, Goverment to Goverment (G2G) -Devlet- devlet- olarak vatandaşlara, şirketlere ve devletlere verilen hizmetlerin doğru bir şekilde ve güvenli bir ortamda gerçekleştirilmesi e-devlet uygulamalarının en önemli öğesidir. Avrupa Birliği (AB) başta olmak üzere, dünyanın gelişmiş ülkelerinde e-devlet uygulamalarında verilen hizmetlerin hızlı ve güvenli bir ortamda gerçekleştirilmesinin yanında, hizmet kalitesini sürekli arttırmak, zaman ve maliyet tasarrufu sağlamak öncelikli amaçtır. Ancak tüm dünyada e-devlet hizmetlerinin ortak sorunu güvenlik endişesidir [8].

Kablosuz iletişim teknolojilerinin gelişmesi sayesinde ortaya çıkan Nesnelerin İnterneti (Internet of Things- IoT), Dünya üzerinde bulunan nesnelerin birbirleri ile haberleşmesini sağlayan ve insan hayatını kolaylaştıran bir teknolojidir. Nesnelerin interneti akıllı ev, akıllı şehir, sağlık, enerji, lojistik ve ticaret uygulamaları gibi pek çok alanda kullanılmaktadır. Günümüzde ev ve iş yerlerindeki güvenlik sistemleri, klima kontrol gibi sistemlerle birlikte buzdolabı, fırın gibi beyaz eşyalar da internete bağlanabilmektedir. Mobil cihazlar marifeti ile hemen her cihaz günümüzde uzaktan izlenebilmekte ve kontrol edilmektedir. Akıllı şehir uygulamalarında şehrin trafik yoğunluğu kontrolü, otoparkların doluluk oranlarının takip edilmesi ve hava kirliliği ölçümleri ve raporlanması gibi alanlarda da IoT teknolojileri kullanılmaktadır [9]. 2020 yılına kadar 50 milyar nesnenin internete bağlı olacağı tahmin edilmektedir [10]. Ancak unutulmamalıdır ki; internete bağlanan cihaz sayısının artması ile güvenlik riskleri de artış göstermektedir.

2016 yılında ortaya çıkan Mirai zararlı yazılımı, çok kısa sürede 2,5 milyon IoT cihazına bulaşmıştır ve 2018'e kadar ölçülen en yüksek boyutta (1.2 Tbps boyutunda) Denial of Service Attack (DDoS) saldırısı gerçekleştirmiştir [11]. Github, Twitter, Reddit, Netflix ve Airbnb gibi çok sayıda yüksek profile sahip web siteleri Mirai zararlısı tarafından hedef alınmış ve bunların her biri zarar görmüştür. Bu zamana kadar IoT'lerin kullanıldığı en büyük saldırı Mirai saldırıları olarak bilişim tarihine geçmiştir.

İnternet günümüzde hemen her sistem için bir erişim ve kontrol aracı olarak kullanılmaktadır. Elektrik üretim ve dağıtım tesisleri, su depolama ve dağıtım sistemleri, doğalgaz dağıtım sistemleri, bankacılık ve finans, ulaşım, sağlık gibi sektörler ve kamu hizmetleri ile bunlara ait alt yapılar, internet ile kontrol edilen, izlenen ve müdahale planlamaları yapılan kritik altyapılar olarak nitelendirilmektedir. Kritik altyapılarda işlenen bilginin gizliliği, bütünlüğü ve erişilebilirliğinin bozulması durumunda büyük ölçekli ekonomik

zarar, can kaybı, ulusal güvenlik açıkları ve/veya kamu düzeninin bozulması söz konusu olabilecektir [12].

Kurumlar her ne kadar teknolojik olarak güvenlik önlemleri almış olsalar da gelişen teknolojinin getirdiği ve her gün değişmekte olan saldırılara karşı yüzde yüz güvenlik sağlanamamaktadır. Symantec tarafından 2017 yılı içerisinde yayınlanan rapora bakıldığında, e-posta ile gelen tehditlerin geride kalan yıllara göre daha çok arttığı görülmektedir. Yine aynı raporda, son 8 yılda veri ihlallerinde 7,1 milyardan fazla kimlik ortaya çıktığı aktarılmıştır [13].

Türkiye'de siber güvenlik çalışmaları kapsamında 2012 Aralık ayında "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" oluşturulmuş ve uygulamaya başlanmıştır. 20 Ekim 2012 tarih ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 28447 sayılı Resmî Gazetede yayımlanmıştır. 11 Haziran 2012 tarihinde 2012/3842 sayılı Bakanlar Kurulunca alınan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin karar ile 28447 sayılı 20/10/2012 tarihli Resmî Gazetede yayınlanarak yürürlüğe girmiştir. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın kabulü; Ulaştırma Denizcilik ve Haberleşme Bakanlığının 18 Şubat 2013 tarihli ve 412 sayılı yazısı üzerine, Bakanlar Kurulu'nca 25 Mart 2013 tarihinde kararlaştırılmış ve 20 Haziran 2013 tarihli 2013/4890 karar ile 28683 sayılı Resmî Gazetede yayımlanmıştır.

Aradan geçen zamanda artan ve değişen güvenlik gereksinimleri ile ortaya çıkan ihtiyaçlar doğrultusunda UDHB'nin hali hazırda var olan ulusal siber güvenlik stratejisini yenilemesi ve 2016 -2019 yıllarını da içine alacak şekilde yeni faaliyet, önlem ve eylemleri belirlemesine ihtiyaç duyulmaya başlanmıştır. 2013 – 2014 Ulusal Siber Güvenlik ve Eylem Planı kapsamında yer verilen kurum ve kuruluşlar ile 10 Mart – 7 Nisan 2015 tarihlerinde değerlendirme toplantıları gerçekleştirilmiş, bir önceki eylem planında yer alan faaliyetlerin ne kadarlık bir kısmının gerçekleştirildiği ve eylem planı uygulanırken yaşanan zorluklar ile geleceğe dönük değerlendirmeler yapılmış siber güvenlik özelinde yapılması gereken faaliyetler ele alınmıştır.

Kamu kurum ve kuruluşları, kritik altyapı işletmecileri, üniversiteler, sivil toplum kuruluşları ve bilişim sektörünü temsilen çok sayıda uzman personelin katılımıyla Ortak Akıl Platformu gerçekleştirilirmiştir. Türkiye'nin siber güvenlik alanında güçlü ve zayıf

yönlerinden yola çıkılarak stratejik hedefleri ve gerçekleştirmesi gereken eylemler tespit edilmiştir.

2016 -2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanırken paydaşlarla birlikte yapılan çalışmalara birçok ülkenin de siber güvenlik stratejilerinde yer alan hedefler, organizasyon yapıları, kamu özel sektör iş birlikleri, Ar- Ge çalışmaları, eğitim gibi alanlarda üretmeye çalıştıkları çözümler detaylı olarak incelenmiştir. Tüm bu çalışmaların çıktısı sonucunda da halen yürürlükte olan 2016 – 2019 Ulusal Siber Güvenlik Stratejisi ve 2016 – 2019 Ulusal Siber Güvenlik Eylem Planı hazırlanmıştır.

Bilgi güvenliğinin tarihçesi, gelişimi ile Türkiye'de ve Dünyada yaşanan önemli bilgi güvenliği olayları ele alınarak Bölüm 2'de detaylı olarak anlatılmıştır. 3. bölümde özellikle 11 Eylül saldırılarından sonra siber güvenlik alanında çalışmalarını arttıran ve oluşturduğu ulusal siber güvenlik politikasını başarılı bir şekilde uygulayan Amerika Birleşik Devletleri'nin eğitim ve farkındalık alanındaki siber güvenlik stratejileri ve çalışmaları incelenmiştir. Avrupa Birliği'nin siber güvenlik stratejilerinde yer alan eğitim ve farkındalık çalışmaları 4. bölümde incelenmiş, Türkiye'nin 2016 -2019 siber güvenlik stratejisi 5. bölümde ele alınarak, 3. bölümde yer alan Amerika Birleşik Devletleri ve 4. bölümde yer alan Avrupa Birliği'nin stratejileri ile karşılaştırılmıştır. Stratejide eğitim ve farkındalığı ön plana çıkarmak için 5.bölümde eğitim ve farkındalık stratejileri hazırlama yöntemleri ele alınarak, farkındalık oluşturulacak kitlelerin tespit edilmesi, eğitim metodolojisinin belirlenmesi ve eğitimlerin planlanmasına ilişkin çalışmalara yer verilmiştir. Tez çalışmasının sonunda elde edilen bilgiler, ülkemizin 2023 siber güvenlik strateji ve hedeflerine katkı sağlayacağı değerlendirilen alan araştırması kısmı 6. bölümde ele alınmıştır. İlkokul 5. Sınıf öğrencileri üzerinde yapılan araştırmanın yöntem, model, veri toplama araçları ve toplanan verilerin değerlendirilmesine ilişkin bilgiler 6. bölümde, bu araştırmadan elde edilen bulgular ise 7. bölümde ele alınmıştır. Çalışmaya ilişkin olarak sonuç ve Türkiye'nin Siber Güvenlik Stratejisine yönelik eğitim odaklı öneriler, 8. ve son bölüm olan Sonuç ve Öneriler başlığı altında toplanmıştır.

Türkiye 2012 ve 2016 yılında yayımlanan Ulusal Siber Güvenlik Stratejilerinin incelenmesi sonucu eğitim ve farkındalık bölümlerine yeterince yer verilmediği görülmektedir. AB ve ABD, hem gençleri eğiterek siber güvenlik alanında yeni projelerin oluşturulmasına imkân yaratmakta, hem de halkın her kesiminden bireyi bilinçlendirerek kişisel

kullanımda bile var olan riskleri düşürmeye çalışmaktadır. Durumun Türkiye'de nasıl ele alındığı araştırmada anlaşılması beklenen en önemli noktadır.

Bu tez çalışması, ulusal siber güvenlik stratejisinin oluşturulmasına katkı sağlamak amacıyla hazırlanmıştır. Kamu kurum ve kuruluşları ile özel sektör çalışanlarına, Kobi ve büyük işletme sahiplerine, karar vericilere, ilk orta ve lise derecesindeki okullarda öğrenci, öğretmen ve velilere verilecek olan farkındalık eğitimleri ile bireysel güvenlik risklerinin azaltılarak, ulusal riskin de bu oranda azalacağı yönündeki amacı ile farkındalık oluşturmak amacıyla yapılmıştır.

Bölüm 2

Bilgi Güvenliği

İnternet kullanılarak gerçekleştirilen işlemlerde güvenli bir ortamın sağlanmasına yönelik ihtiyaç ve bu ortama dair güven oluşturulması isteği her an daha fazla hissedilmektedir. Bunun temelinde internetin ekonomik toplumsal ve kişisel iletişim ve veri akışı için en fazla kullanılan araç olması ancak bir o kadar da tehditlere açık bir mecra olması yatmaktadır. Hal böyle olduğundan internet ve burada güvenliğin sağlanmasına ilişkin kaynaklar ve faaliyetler; yeni teknoloji, süreç ve iş modellerini oluşturmaktadır. Bilgi toplumu dönüşümü, bireysel ve toplumsal risklerle beraber bilişim suçlarını, siber saldırıları, veri sızıntılarını ve bunlara benzer kişi ve kurumlara telafisi zor zararlar verebilecek tehditleri doğurmaktadır. Bu tehditler ekonomik kayıplar, kişilerde güven eksikliği ve hizmet kesintileri gibi endişeleri ortaya çıkarmaktadır. Kişisel verilerin korunması, bilişim suçlarıyla mücadele ve güvenli internet gibi alanlarda bilgi güvenliğini korumak maksatlı stratejiler oluşturma ihtiyacı oluşmuştur [14].

Bu noktada öncelikle bilginin ne olduğunu kavramak, konunun bütünlüğünü anlamak açısından önem taşımaktadır. Bilgi kelimesinin sözlük anlamı,

i "İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat

ii Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf

iii Bilim,

iv İnsan zekasının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf" şeklindedir [15].

Russel bilgi ve bilmek kavramlarını birlikte incelemiş ve her iki kavram için keskin bir anlam ayrımı yapmanın çok mümkün olmadığını belirtmiştir. Araştırmacı bilgiyi tanımlamaya çalışmak yerine bilgi olarak hangi verilerin adlandırılması gerektiğini belirtmiştir. Bir başka deyişle kişiler bilgi nedir diye sormak yerine, ne bilgidir diye sormalıdırlar. Araştırmacıya göre bilgi, "kâğıt ya da başka ortamlar üzerine kaydedilmiş, anlaşılabilen ve iletilebilen veriler topluluğudur". Ayrıca yazar bilginin "zihnin herhangi bir biçimde resmi veya gayri resmi olarak iletilen, kaydedilen, yayınlanan fikirlerin gerçek ve hayali ürünleri olduğunu" da belirtmektedir [16].

Bilgi güvenliği için dijital ortamlarda bulunan verilerin çeşitli yasak yollar ile bozulmasını engellemek açıklaması yapılabilir. Buna açıklık getirilecek olursa, bilgiye erişimi olmaması gereken tarafların buna müdahale etmesinin önüne geçmek için alınan tüm önlemleri bilgi güvenliği kapsamında düşünmek mümkündür. Bilginin yalnızca depo edilmesi esnasında değil, işlenmesi ve transfer edilmesi esnasında da güvenli biçimde faaliyetlerin gerçekleştirilmesi ve tam bir güvenli ortam sağlanmasıdır [17]. Bilgi güvenliği gizlilik, bütünlük ve erişilebilirlik gibi unsurlarla ileride daha detaylı olarak açıklanacaktır.

2.1 Bilgi Güvenliği Tanımı

Bilgi güvenliği son yıllarda kendi başına bir bilim olarak görülmeye başlanmıştır. Bilginin güvence altına alınması pratiği, sır saklamaya ihtiyaç duyulduğunda ortaya çıkmıştır. Aslında insanlar tarihin her döneminde kimi bilgileri saklamak istemişlerdir. Örneğin gıdanın yeri, temiz suyun bulunduğu yer ya da yerleşime uygun alanlar insan topluluklarının rakip olan diğer topluluklardan sakladığı bilgilerdir. MÖ 1500 yılında bir Mezopotamya tableti üzerinde şifreli şekilde yazılmış çömlek yapımı formülü bulunmuştur. Bu bulgu, tarihin her döneminde bilginin önemli bir kaynak olduğunu bize göstermektedir. Ayrıca bu kanıt kriptografinin kayıtlara geçtiği ilk kullanımı olarak kabul edilmektedir. Bilgi güvenliğinin stratejik önem kazanması daha çok İkinci Dünya Savaşı dönemine denk gelmektedir. Bu dönemde bilgi güvenliği, askeri ve diplomatik amaçların gerçekleştirilmesi için dikkat edilen bir unsur olmuştur. Küreselleşme ile bilgi, politik, diplomatik ve ticari güç anlamına gelmeye başlamıştır.

Bilgi güvenliği, bilgiye izni olmayan kişilerin erişimini ve bilginin bozulmasını önlemektir. Bilginin bilinçsiz ya da erişim izni olmayan kişiler tarafından ele geçirilmesi, sızdırılması,

yok edilmesi, değiştirilmesi ya da yayılması onun güvenliğinin olmadığını gösterecektir. Bilgi güvenliğinden söz etmek için onun prensiplerinden de söz etmek gerekmektedir [18]:

i Gizlilik: bilgiye yalnızca yetkili kişiler tarafından erişilmesi onun gizliliği anlamına gelmektedir. Gizliliği sağlamanın en kolay yolu bilgiyi şifrelemektir.

ii Bütünlük: bilginin yetkisiz kişiler tarafından değiştirilememesi bütünlüğü ifade etmektedir. Örneğin elektronik imza ya da açık anahtar yapısı ile bilginin bütünlüğü korunabilmektedir.

iii Erişilebilirlik: bilgiye ihtiyaç duyulduğunda yetkili kişilerin ona ulaşabilmesi anlamına gelmektedir.

iv Loglama: bilginin hesap verilebilirliğini temsil eden terimdir. Bilginin elde edilmesi, işlenmesi, arttırılması gibi faaliyetlerin tamamının şeffaf olması gerekmektedir. Loglama diğer tüm faaliyetlerin de düzenli şekilde devam etmesine yardımcı olmaktadır.

v Kimlik Doğrulama: bilgiye erişme esnasında kişinin gerçekten yetkili olup olmadığı, bunlara bir insan ya da makine tarafından erişilip erişilmediğini kontrol etmek gerekmektedir.

vi İnkâr Edilemezlik: log kayıtları, bilginin inkâr edilemezliğini desteklemektedir. Bir bilgi var ise onun varlığı reddedilemeyecektir. İnkâr edilemezliğin sağlanması için bütünlüğü korunmuş, tutarlı log kayıtlarının tutulması mekanizması gerekmektedir.

vii Güvenilirlik: bilgi, başka bilgilerin üretilmesi için kullanılmaktadır. Özellikle bilişim sistemleri ile üretilen bilgilerin, elde edilmesi beklenen bilgiler ile tutarlı olması beklenmektedir ve buna güvenilirlik adı verilmektedir.

2.2 Bilgi Güvenliğinin Gelişimi

Tarih boyunca bilgi, insanın en değerli hazineleri arasında olmuştur. Bilginin güç getirdiğinin fark edilmesi neticesinde bilgiye verilen değer artmış, bilginin doğru saklanması gündeme gelmiştir. Ancak bu noktada bilgi güvenliğinin nasıl geliştiğine de açıklık getirmek gerekmektedir.

Bilgi güvenliğinin neden önemli olduğunu kavrayabilmek adına öncelikle doğru zamanda ve doğru şekilde bilgi almanın önemini kavramak gereklidir. Bilgi sayesinde ilkel insanlar

hayatta kalmayı başarmışlardır ve kendi topluluklarını hayvanlardan ve diğer insanlardan korumak, enerji ve besin kaynaklarını kaybetmemek ve temel ihtiyaçlarını karşılayabilmek için bilgiyi güvende tutmaları gerektiğini anlamışlardır [19].

İnsanlar arası iletişim ve etkileşimin gelişmesi ve bilgi ile bilinçliliğin artması, bilgi güvenliği için ek önlemler alınması gerekliliğini de ortaya çıkarmıştır. Bununla ilgili ilk önemli çalışmalardan biri Caesar şifrelemesidir. Ancak bu noktada öncelikle şifreleme ve kriptolojinin ne olduğunu anlamak önemlidir. Şifreleme, kısaca alıcı ve göndericinin çözebildiği bir tür mesajlaşma dili olarak nitelendirilebilecektir. Kriptoloji ise bir şifreleme bilimidir. Kriptolojide mesajların gizlenmesi için belirli algoritmalar oluşturulmaktadır. Bu bir çeşit yeni dil anlamına gelmektedir ve tarihte ilk örneklerden biri Caesar Şifresidir. Bu oldukça basit bir algoritmadır. Kullanılan alfabede her harfin kendisinden sonraki ya da belirli aralıktaki bir diğer harfle yer değiştirmesi ile mesaj hazırlanmaktadır [20]:

ALFABE :	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
ŞİFRE :	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C

Şekil 2.1: Caesar Şifreleme Örneği.

Kaynak: Topaloğlu ve ark., 2016: 294

Caesar şifresi Roma döneminde ortaya çıkmıştır ve ordu bilgilerinin dışarıya açılmasını önlemek için Büyük Roma İmparatoru Julius Caesar, komutanlarıyla kendi geliştirdiği bir yerine koyma sistemini kullanarak iletişim kurmuştur. Günümüz için çok basit bir şifreleme yöntemi olsa da Caesar şifreleri dönemde ihtiyaçları karşılamıştır [21].

Kuşkusuz devlet yönetimlerinin sorunsuz şekilde devam etmesi için de bilgi oldukça önemlidir. Özellikle savaş dönemlerinde, devletin savaşma biçimine ilişkin bilgileri ve planlarının iyi korunması, o devlet için hayati önem taşımaktadır. İkinci Dünya Savaşı esnasında teknolojinin de gelişmesi ile birlikte eski usul yöntemlerin yerini yeni nesil bilgi güvenliği sistemleri almaya başlamıştır ve Enigma buna en iyi örnektir. Almanlar tarafından bilgi yönetimi ve güvenliği için kullanılan Enigma şifrelerinin diğer ülkeler tarafından çözülmesi ve bu çözüm neticesinde Atlantik'teki Alman "U-boat" savaşında, Normandiya Çıkarması'nda ve Afrika Çöl Savaşları'nda müttefiklerin çok büyük avantajlar elde etmiş olmaları durumun önemini de gözler önüne sermektedir [22].

Enigma, banka ve iş dünyasında gizliliğe ilişkin taleplerin artması neticesinde 20.yüzyılın başlarında Alman mühendis Arthur Scherbius tarafından geliştirilmiştir. Enigma (bilmece/muamma anlamına gelmektedir) adı verilen rotorlu bir kripto cihazı sayesinde bilgiler şifreli hale getirilmiş, bilgi güvenliğinde en önemli teknolojik gelişmelerden biri olmuştur. Cihaz önceleri oldukça ağır olmasına karşın üreticisi üzerinde çalışarak kısa sürede onu portatif ve daha kullanışlı hale getirmiştir. Her ne kadar iş dünyası için geliştirilmiş olsa da Enigma ordudan daha çok ilgi görmüş ve cihaz Alman ve İsviçre ordularında, İspanyol İç Savaşı'nda ve İtalyan donanmasında kullanılmıştır [22].

Enigma'nın yarattığı bilgi güvenliği başarısızlıkları neticesinde ordular başta olmak üzere hemen her sektörden kullanıcılar yeni güvenlik sistemleri arayışına girmişlerdir. Manyetik teyp kullanarak verileri depolayan UNIVAC bilgisayarlarının üretilmesi, kriptolojiye de yeni bir bakış açısı getirmiştir. Çünkü bilgiler artık bilgisayarlarda toplanmaya başlamış ancak elektromanyetik saldırılara da daha açık hale gelmişlerdir. Amerikan Savunma Bakanlığı bilgilerini güvende tutmak için ARPANET (The Advanced Research Projects Agency Network) birimini kurmuşlar ve böylelikle internetin de ilk adımlarını atmışlardır [23].

Aslında ARPANET, ülkedeki askeri birimlere ait bilgisayarlar arasında iletişim kurulmasını sağlayan ve bu sayede ucuz ve güvenilir bilgi akışını gerçekleştirme imkanı yaratan bir sistem olarak kurulmuş; soğuk savaş döneminde ABD'nin savunmasının yapı taşlarından biri olmuştur. Bu sistem bilgisayarlardan birine bir şey olsa dahi sistemin çökmeyeceği şekilde ve birimler arasında iletişim ve koordinasyonu sürekli kılacak biçimde tasarlanmıştır. Zamanla ağa başka bilgisayarların eklenmesi de mümkün hale gelmiştir. Farklı bilgisayarların sisteme katılması, iletişim güçlüklerini de beraberinde getirdiğinden, araştırmalar ortak bir dilin nasıl yaratılacağı yönüne kaymış, TCP/IP (Transmission Control Protocol / Internet Protocol) kullanılmaya başlanmıştır [24].

İnternetin yaygınlaşması ve şifrelerin daha hızlı çözülebilme riskinin artması neticesinde 64 bit blok uzunluğunda, 56 bit anahtar boyu olan bir blok şifreleme Algoritması olan DES (Data Encryption Standard- Veri Şifreleme Standardı) ABD'nin şifreleme standardı olarak kabul edilmiş ve dünyanın en güvenilir şifreleme yöntemlerinin algoritması haline gelmiştir. IBM firmasının çalışanları tarafından ortaya çıkarılan bu algoritma karşılıklı olarak mesaj alıcısı ve vericisinin arasına başkalarının girmesini önlemeye yönelik bir çalışma olmuş ve o zamana dek mesaj iletilerindeki şifreleme yöntemlerine yeni bir boyut

kazandırarak literatüründe dikkatini çekmiştir. Algoritmanın başarısı ayrık algoritmaların matematiksel olarak çözülmesinin zor olmasından kaynaklanmış, dönemin ilk açık anahtarlı şifreleme yöntemi olmuştur. Bu sayede diğer kriptologların da ilgisi artmış ve şifreleme bir bilim dalına dönüşmüştür. Koblitz ve Miller tarafından eliptik eğri, Shamir ve Adelman tarafından da RSA adlı yeni şifreleme sistemleri çıkarılmıştır. Dönemde hiçbirine DES kadar güvenilmemiş fakat 1990'lara gelindiğinde algoritmanın çok sayıda saldırıya uğraması ile itibarını kaybetmeye başlamıştır. Ardından Mitsuri Matsui tarafından doğrusal kriptoanalizi keşfedilmiş ve DES'in kolaylıkla kırılabileceği görülmüştür. Bunun neticesinde DES kullanımı hızla düşmüştür [25].

Standards and Technology-(Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından gerçekleştirilen yeni nesil şifreleme yarışmasının bir ürünü olarak ortaya çıkmıştır. 2001 yılında bu yarışmadan ödül alan iki kriptolog tarafından Rijndael adlı bir şifreleme algoritması oluşturulmuş ve bu algoritma AES (Advanced Encryption Standard- Gelişmiş Şifreleme Standardı) olarak uluslararası bir şifreleme standardına dönüştürülmüştür. Bugün pek çok ülke ve kuruluşta AES standartlarına uygun şifrelemeler kullanılmaktadır [22] [26].

2.3 Türkiye'de Yaşanan Bilgi Güvenliği Olayları

Bilgi güvenliği son yıllarda hem kişilerin hem kurumların hem de ülkelerin en fazla önem verdiği konular arasında yerini almıştır. Elbette bunun en önemli nedeni günümüzde hemen her işlemin bilgisayarlar ve internet aracılığı ile yapılmasıdır. Bankacılık işlemlerinden kişisel verilerin korunmasına, kurumların işletme bilgilerine, üretim planlarına ve ülkeler arasındaki ilişkilere dek hemen her işlem bilgisayarlar aracılığı ile hızlı olarak gerçekleştirilmektedir. Ancak bu noktada bilgi güvenliğinin siber saldırılara karşı korunmasız olma riski ortaya çıkmaktadır.

Türkiye, bilgisayar sistemlerine ilişkin bilgi güvenliği konusunda maalesef dünyanın oldukça gerisindedir. Sazan avlama, virüs korumaları ve bunlara benzer durumlara ilişkin literatür bilgisi yok denecek kadar azdır. Elbette konuya ilişkin araştırmaların azlığı, bilgisizliği ve koruma açıklıklarını da beraberinde getirmektedir [27].

Buna karşın yapılan anket uygulamaları ve özellikle sokak röportajları, Türkiye'de insanların bilgi güvenliği konusunda kısa zaman içinde daha fazla dikkatli hale geldiğini göstermektedir. 2017 yılında yapılan bir araştırmada, Türk şirketlerinin yüzde 52'sinin bilgi güvenliğine ilişkin yatırımlarını son 3 yıl içinde arttırdığı görülmüştür. Yapılan güvenlik yatırımları ile son bir yılda tespit edilen güvenlik risklerinin yüzde 26 oranında arttığı görülmüştür. Aynı araştırmanın sonuçlarına göre Türkiye'de 2017 yılından itibaren faaliyet gösteren şirketlerin yüzde 61'i güvenlik için biyometri, yüzde 59'u ise kesinlikle açık kaynaklı yazılım kullanmaktadır. Yine bu şirketler güvenlik için ek olarak siber güvenlik amaçlı satılan yazılımlar ile büyük veri analiz sistemleri satın almaktadır [28]. Kuşkusuz bu bilinçlenme üzerinde yaşanan olumsuz olayların etkileri büyüktür.

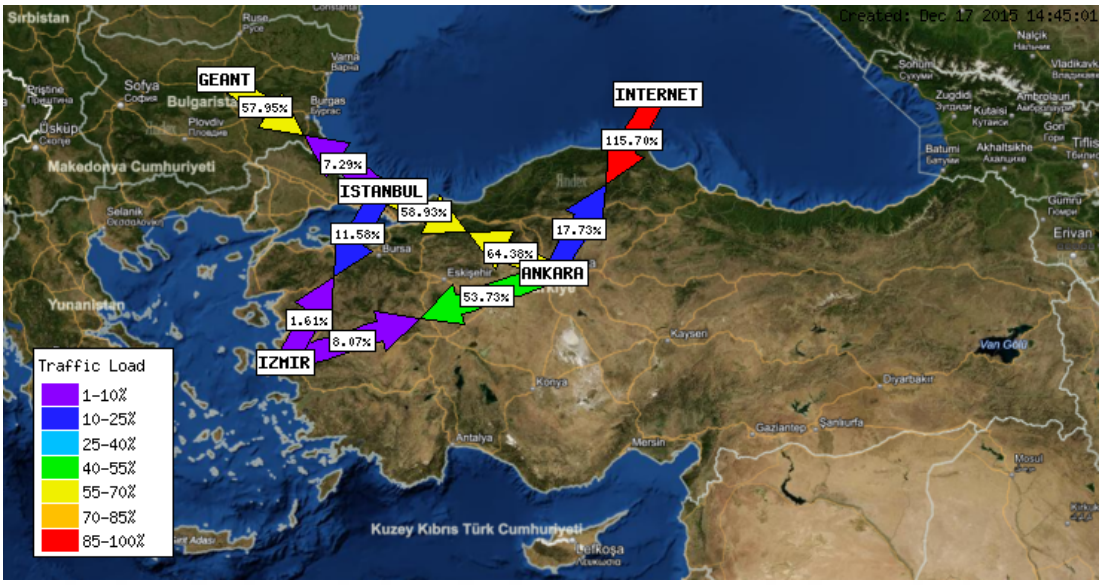
2.3.1 Atatürk Havalimanı Zararlı Yazılım Ocak 2009

30 Ocak tarihinde dünya genelindeki pek çok kurum ve Atatürk Havalimanı sistemleri, zararlı bir yazılım ile karşılaşmış ve zarar görmüştür. Yapılan araştırmalar, havalimanı bilgisayar sistemine 'Conficker' isimli bir virüsün yayıldığını göstermiştir. Bu kötü yazılım, kısa sürede pek çok dosyaya yayılabilmekte ve onarılması güç ve hatta imkansız zararlar verebilmektedir. Dönemde, özellikle dış hatlar terminalinin düzenlenmesi için kullanılan sistemler büyük zarar görmüştür [29].

Virüsün sisteme girmesi ile havalimanı dış hatlar terminalinde yolcu ve bagaj işlemlerini yürüten sistemlerde kayıplar yaşanmıştır. Havaalanının işletici firması TAV tarafından yapılan açıklamada, virüsün temizlenmesi için gereken sürede bagaj ve yolcu alım işlemlerinin el ile yapıldığı ve bu durumun zaman sorunları doğurduğu belirtilmiştir [30]. Virüsün havaalanı sistemlerine girmesinin nedeni işletici firmanın Dış Hatlar Terminalinde "SITA CUTE" adlı uluslararası bir bilgisayar firması tarafından işletilen sistemin kullanılmasıdır. Bu sistemin kullanıldığı dünya genelindeki tüm havalimanlarında aynı sorun ortaya çıkmış ve büyük panik yaşanmıştır. "Ağa karışmış solucan" olarak tanımlanan bu virüs nedeni ile Atatürk Havalimanına ait 400'den fazla sistem merkezinde tarama ve temizleme işlemi gerçekleştirilmiştir [31].

2.3.2 Nic.Tr DDoS Saldırısı Aralık 2015

14 Aralık 2015 tarihinde tam öğlen saatinde, ".tr" uzantılı alan adlarına erişimlerde yavaşlıklar ve erişim problemleri yaşanmaya başlanmıştır. Yurt içi ve yurt dışında beş ayrı bölgede barındırılan 6 sunucu, DDoS saldırısı ile karşı karşıya kalmıştır. UlakNet'in anlık omurga verileri göstergesine göre, kuzey hattından 35 -50 Gbps boyutunda ve kapasitenin üzerinde bir yüklenme oluşmuştur.

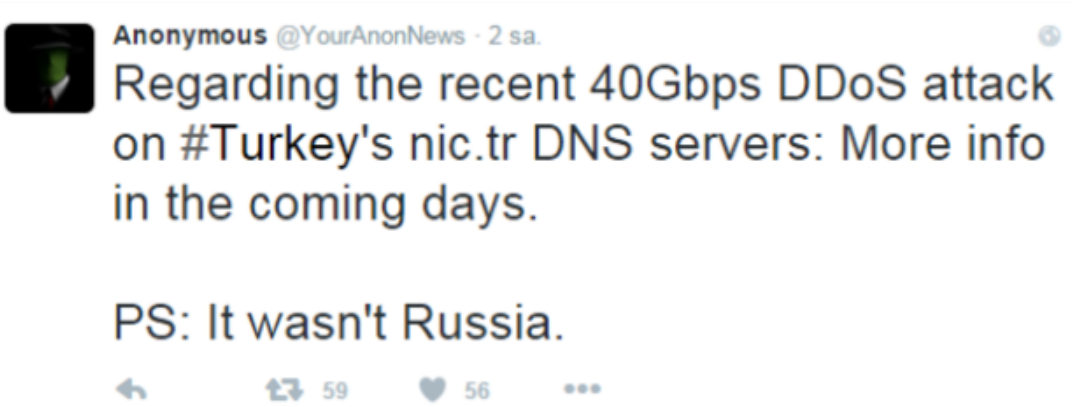


Şekil 2.2: ULAKBIM Anlık omurga verileri 14 Aralık 2015.

14 Aralık günü RIPE tarafında yetkili olan Romeo Zwart tarafından bir açıklama yayınlandı. Açıklamada, "saldırının UTC 08:00 civarında başladığı RIPE tarafından çeşitli önlemlerin alındığı ve alınan bu önlemlerin bir süre etkili olduğu ve saldırının büyüklüğü karşısında önlemlerin yetersiz kaldığını, gelen saldırının sahte IP adresleri üzerinden spoof yapmakta olduğu konuyla ilgili olarak servis sağlayıcılar tarafında gerekli önlemlerin alınmasının önem arz ettiğini ve kaynak adres doğrulaması için BCP-38 uygulanmasının ve bu yolla şebekelerin zorlanmasının azaltılması gerektiği bilgisine yer verildi" [32].

Alan yazınında bu saldırıların nedeni olarak dönemde yaşanan Türkiye ve Rusya gerilimi gösterilmiştir. Türkiye'nin hava sahasını ihlal etmesi gerekçesi ile bir Rus askeri uçağını düşürmesi, ülkelerin siber ortamda bir savaşa girmesi için bir neden olarak kabul edilmektedir. Darıcılı ve Özdal'a göre, bu saldırının amacı Türkiye'nin ekonomisini zedeleyecek biçimde finansal faaliyetler gösteren kurumların işlemlerinin aksatılmasıdır [33]. Ancak

alan yazınının aksine, saldırıyı Anonymous adlı grup üstlenmiş ve saldırı gerekçesi olarak Türkiye'nin IŞID'a destek vermesini göstermiştir:



Şekil 2.3: Nic.Tr DDoS saldırısı hakkında anonymous tarafından yapılan twitter açıklaması.

"Türkiye Nic.Tr DDoS Saldırılarıyla ilgili olarak önümüzdeki günlerde daha fazla bilgi verilecektir. Not: Rusya Değildi" [34].

DNS kayıtlarının tutulduğu sunucuların IP adreslerine ulaşımın engellenmesi maksadıyla yurt dışı operatörler yönünde Border Gateway Protocol (BGP) kaydı yollanmıştır. Geçici çözüm için yalnızca yurt içi sunucular açık tutularak, yurtdışı sunucular kapatılmış; bu sayede saldırının gücünü kaybetmesi sağlanmıştır [35].

21 Aralık tarihinde Nic.TR tarafından saldırıya ilişkin bir açıklama yayınlanmıştır. Açıklamada; "Bu saldırı, .tr Alan Adaları'ndan ilgili IP adreslerine ulaşılmasını engellemek amacıyla, sahte ağ trafiği üretmek de dahil olmak üzere, DNS sunucularımıza doğru yoğun ağ trafiği yollanması şeklinde ülke dışındaki kaynaklar tarafından organize bir şekilde gerçekleşmiştir" denilmiştir [36].

Ayrıca Nic.TR tarafından yapılan açıklamanın I maddesinde, "Saldırı, sahte ağ trafiği üreterek ülke dışındaki kaynaklar tarafından gerçekleştirildiği için, bu tip saldırıların tek çözümü saldırı oluştuğunda ülkenin İnternet girişinin ana kapıları ve arterlerinde korunma sağlamaktır. Bu sözü edilen korunma biçimi ve önlemleri şu anda sürmektedir ve saldırının ileride tekrarlanması halinde de bu önlemlerin Telekom operatörlerimizce alınacağı açıktır" ifadelerine de yer verilmiştir [37].

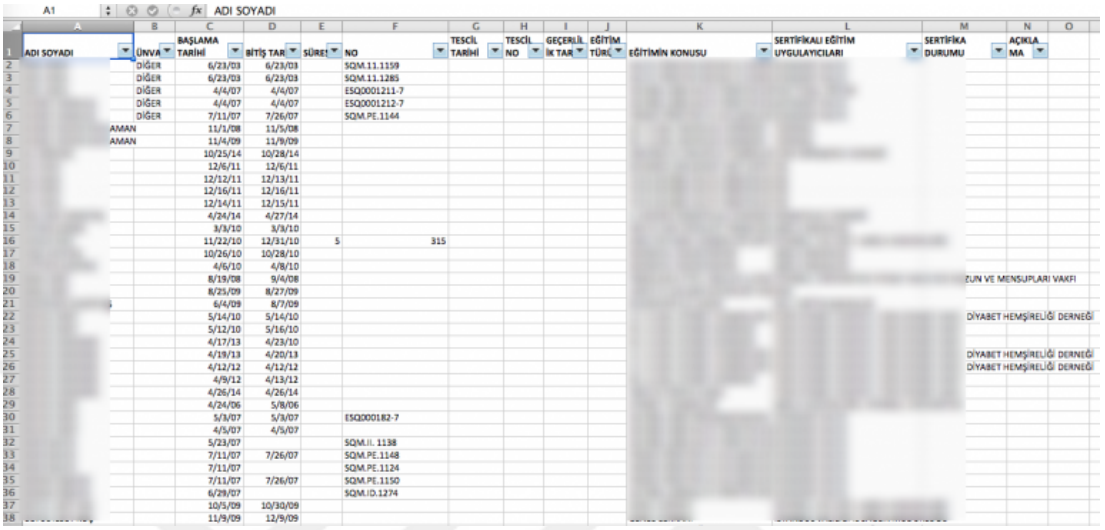
2.3.3 Sağlık Bakanlığı Hastanelerine Yönelik Siber Saldırılar Mayıs 2016

17 Mayıs 2016 tarihinde sabah 09:30 sıralarında Sağlık Bakanlığı'na bağlı Devlet Hastaneleri'nin veri tabanlarına sızan hacker grubu hastanelerin veri tabanlarındaki tüm veriyi kopyalayarak veri tabanlarını silmiştir. Hastanelerde sistem üzerinden verilen hizmet durmuş; veriler yedeklerden geri yüklenmeye çalışılmış fakat saldırganların verileri geri yüklemeyi de engellediği görülmüştür. Siber saldırıya uğrayan Devlet Hastanelerinin kayıtları saldırı sürecinde manuel olarak aldıkları belirtilmiştir [38].

Çok sayıda hastanın kayıtlarının ele geçirildiği ve internetten paylaşıldığı, saldırının Anonymous grubu tarafından gerçekleştirildiği ve Hollywood'da bulunan Presbyterian Sağlık Merkezi ve Methodist Hastanesi'nin veri tabanlarına yapılan siber saldırıya karşılık olarak yapıldığı bir video mesajı ile Youtube üzerinden paylaşılmıştır. Sağlık Bakanlığı 18 Mayıs 2016 tarihinde yaptığı resmi açıklamada, Bakanlığa bağlı Diyarbakır, Siirt, Tekirdağ ve Kocaeli illerindeki kimi hastanelerin bilgisayar sistemlerine siber saldırı girişiminde bulunulduğunu, yapılan eylemden yalnızca Diyarbakır ilinde bulunan hastane sisteminin bir kısmının olumsuz etkilendiğinin fakat var olan yedekler sayesinde sorun oluşmadığının açıklaması yapılmıştır [39]. Diğer taraftan saldırının yapıldığı aynı günün akşamı, Anonymous hacker grubu Twitter hesabından yaptığı bir açıklama ile saldırıyı reddetmiştir:

Şekil 2.4: Anonymous twitter açıklaması.

33 hastaneden sızdırılan 2 Gb büyüklüğündeki hassas verilerde, tüm hastaların ve doktorların kayıtlarına erişilmiş ve bunlar ifşa edilmiştir. Yayınlanan video Youtube tarafından kaldırılmış, dataların yüklendiği adresler de erişilemez duruma getirilmiştir. Datanın kimlerin eline geçtiği ve hangi boyutlarda olduğu halen tespit edilememiştir.



Şekil 2.5: Sağlık bakanlığı hastanelerinden İfşa edilen veri örneği.

2.4 Dünya'da Yaşanan Siber Güvenlik Olayları

Dünyada internetin ve bilgisayar kullanımının yaygınlaşması, insanların hayatını kolaylaştırmanın yanı sıra bilgi hırsızlığına ilişkin riskleri de arttırmaktadır. Bilgilerin ele geçirilmesi kişisel verilerden başlayarak devlet sırlarına kadar hemen her türlü bilginin dışarı sızması ya da zarar görerek kullanılamaz hale gelmesi siber güvenlik olayları olarak özetlenebilecektir. Dünya genelinde şifreleme konusunda dev projeler yapılsa da, zaman zaman kurumlara ciddi sorunlar yaratan bilgi güvenliği sorunları olmuştur.

Cüneyt Kırlar, ne kadar önlem alınırsa alınsın, güvenlik sınırlarının hala bulanık olduğunu, bir tehdidin ne zaman ortaya çıkacağının bilinmediğini ve sürekli güvenlik amaçlı yazılımların takip edilmesi gerektiğini vurgulamaktadır. Kırlar, yalnızca önlem almanın da güvenliği sağlamayacağını, yasalar ve yaptırımların da sürekli ihtiyaca cevap verir nitelikte geliştirilmesi gerektiğini de belirtmektedir. Risk analisti güvenlik olaylarının neden, ne zaman ve hangi alanlarda yapıldığına ilişkin takiplerin de unutulmaması gerektiğini sözlerine eklemektedir. Örneğin 2013 yılında dünya genelinde yaşanan siber güvenlik

olaylarının yüzde 35'i web uygulamaları ile yüzde 22'si siber casusluk aracılığıyla, yüzde 9'u kayıp ve çalıntı kartlar ile yüzde 8'i şirket içi kötüye kullanım ile gerçekleşmiştir [40].

2.4.1 Estonya Saldırısı Nisan 2007

2007 yılının Nisan ayında, Estonya Hükümeti, ülkenin web sitelerinin üç haftadır yoğun saldırı altında olduğunu ve bundan Rusya'yı sorumlu tuttuğunu söylemiştir. Siber saldırı 27 Nisan 2007'de, Tallinn'de II. Dünya Savaşı esnasında Alman ordusunun karşısında savaşırken ölen Rus askerlerin anısına yapılmış Meçhul Asker anıtının, bulunduğu yerden sökülerek bir başka yere taşınmasıyla başlamıştır. Faşizme karşı mücadeleyi temsil ettiğini savundukları anıtın taşınmasına karşı çıkan Rus azınlığın protesto gösterileri sırasında bir kişi hayatını kaybetmiş, çok sayıda kişi yaralanmış ve binden fazla kişi de tutuklanmıştır. Estonya Hükümeti saldırıların, olayların hemen ardından başladığını ifade ederek, olayları saldırının gerekçesi olarak göstermiştir [41] [42].

Çok büyük oranda internete bağımlı olan Estonya'da Cumhurbaşkanlığı, bakanlıklar, siyasi partiler, ülkenin en büyük bankaları, iletişim kurumları gibi çok sayıda kurum ve kuruluşa DDoS hizmet durdurma saldırıları yapılmış, hackerlar, kullandığı binlerce zombi bilgisayar ile Estonya web sitelerine milyonlarca istek göndermişlerdir. Estonyalı uzmanlar saldırının dünyanın her bir yanından geldiğini ancak en başlarda bazı saldırganların adreslerinin belirlendiğini ve bu adreslerin büyük çoğunluğunun Rus kamu kuruluşları olduğunu açıklamışlardır [41]. Saldırı 9 Mayıs'a kadar sürmüş; 3 Mayıs'ta zirveye ulaşmıştır. Saldırılar, özellikle Rusya'nın Zafer Günü kutlamaları olan 8 – 9 Mayıs tarihlerinde de büyük bir yoğunlukla devam etmiştir. "Kağıtsız devlet" olarak nitelendirilen Estonya çok büyük ölçüde internete bağlı olduğundan saldırıların boyutları çok büyük olmuştur. Tüm bankacılık hizmetleri, vatandaşlık hizmetleri, şirket kurulumları, hatta parlamento seçimleri bile internet üzerinden yapılan bu ülkede saldırılar esnasında hayat adeta durma noktasına gelmiştir. NATO sözcüsü James Appathurai, Estonya hükümetinin talebi doğrultusunda kendilerine teknik yardımda bulunulduğunu açıklamıştır [41] [43] [42].

2.4.2 Sony Saldırısı Aralık 2014

Sony Pictures Entertainment yapım stüdyosu tarafından Kuzey Kore lideri Kim Jong Un'a karşı bir suikastı konu eden "Röportaj" isimli bir film hazırlamış, buna karşılık Kuzey Kore, bu filmi aşağılayıcı bulmuş ve filmin yayınlanmadan yok edilmesi için şirkete siber saldırı düzenlemiştir. Bu hackerlik olayının ardından Sony'nin PS3 sistemini kıran hackera dava açması, dünya genelinde diğer hackerlerin tepkisine neden olmuş, firma siber saldırıların açık hedefi haline gelmiştir. Gerçekleşen saldırıları aktivist bir hacker grup üstlenmiştir. Sony bu saldırı neticesinde filme yönelik başlatılan saldırıların siber güvenlik sorunundan çok ifade özgürlüğüne karşı bir saldırı olduğunu belirtmiştir. Ancak saldırının siber güvenlik boyutları da oldukça ağırdır. Süreç neticesinde yine Sony'nin açıklamalarına göre 100 milyon dolardan fazla zarar verilmiş ayrıca PlayStation ağında bilgileri bulunan 11 milyon kullanıcının kişisel bilgileri ele geçirilmiştir. Saldırı sonrasında Barack Obama bir açıklamasında, ABD'nin diktatörlerin sansür uyguladığı bir ülkeye dönüşmeyeceğini, buna izin verilmeyeceğini belirtmiştir [42].

Sony saldırısı ilk defa Ananymous adının da duyulduğu saldırıdır. Bu grup Sony'ye saldırmanın hemen ardından ABD ordusuna hizmet satışı yapan Lockheed Martin firmasının temel bilgi ağına saldırı gerçekleştirerek dünya gündemine yerleşmiştir. Bu aktivist hacker grubu hakkında araştırmalar yapıldığında geçmişte İrlanda seçimlerine de müdahale ettikleri görülmüştür. Arap Baharı döneminde de Tunus'lu hackerlar ile iş birliği yapan bu grup Tunus devletine ait web sitelerine de saldırmış, 8 siteyi bir süreliğine etkisiz hale getirmişlerdir. Bu grup daha sonra Wikileaks ile çalışmak istemeyen Visa, MasterCard ve PayPal'a da savaş açmış ve bu şirketlerin web sitelerini hacklemiştir. Grup, Burger King'ten satın aldıkları bir menünün tadını beğenmedikleri gerekçesiyle, şirketin bir sosyal medya hesabını da ele geçirmiş ve Burker King'in en büyük rakibi olan Mc Donald'sın logoları ile web sayfası tasarımını değiştirmiştir. Grubun aktivitelerine ve saldırılarına bakıldığında genel olarak ABD ve ABD menşeli şirketlere zarar verdiği görülecektir ki bu durum ABD'nin siber güvenlik stratejilerini yenilemesi gerekliliğini gözler önüne sermiştir [44].

2.4.3 ABD DDoS Saldırısı Ekim 2016

2016 yılında Çin ve Rusya üzerindeki hackerler tarafından yapılan ABD DDoS saldırısı, tarihin en büyük siber saldırıları arasında yerini almıştır. Distributed Denial of Service (Dağıtık Hizmet Engelleme) şeklinde adlandırılan bu saldırı türü, aynı anda gönüllülük esasına dayanan pek çok kullanıcı tarafından gerçekleştirilmiş, dev bir işlemci gücüne sahip olunduğu için saldırıyı önlemek ve savunma yapmak ABD için imkânsız hale gelmiştir. Toplamda 14 milyondan fazla IP'nin kullanıldığı saldırıda ABD sosyal medya sitelerine sahip olan şirketler, Whatsapp ve benzeri mesajlaşma uygulamaları, dünyanın en büyük DNS servis sağlayıcısı, siber saldırı ölçüm servisi NorseCrop ve dijital oyun platformu olan Origin ve Steam gibi devler etkilenmiş, şirketler uzun saatler işlem yapamamış ve kullanıcılarına hizmet verememişlerdir [45].

Saldırı esnasında Twitter, Facebook, SoundCloud, Spotify ve Shopify gibi web sitelerine dünya genelinde erişim durmuştur. Tehdit istihbaratı yapan firma Flashpoint, saldırının Mirai adındaki bir zararlı yazılım ile gerçekleştirildiğini ve özünde saldırının ABD menşeli DYN isimli DNS firmasına yapıldığını; pek çok popüler uygulama ve web sitesinin DYN'nin servislerini kullanmasından dolayı etkilendiklerini duyurmuştur [46].

Mahjabin ve arkadaşları, DYN müşterisi olan 3500 web sitesi ve uygulamanın bu saldırıdan olumsuz etkilendiğini belirtmişlerdir. Bu saldırı esnasında yalnızca ABD'nin dijital alanda savunmasız olduğu mesajı verilmemiş, aynı zamanda sistemlerinin açıklıkları ortaya çıkarılmış ve 70 milyondan fazla kullanıcının isim, şifre ve kredi kartı bilgileri de ele geçirilerek büyük bir panik ortamı oluşturulmuştur. Elbette bunun yanı sıra saldırıya uğrayan DYN firmasının imajı zedelenmiş, firma online platformlarını aylarca kullanamamış itibarın yanı sıra çok büyük maddi kayıplar da vermiştir [47] [40]. Yönak'ın BBC haberine göre saldırının Amerika'ya maliyeti 7 milyar dolardan fazladır [48].

Bölüm 3

Amerika'nın Siber Güvenlik Stratejilerinin İncelenmesi

Amerika, soğuk savaş dönemi başta olmak üzere 1990 sonrasında hızla artan internet kullanımını hem bir avantaj hem de bir tehdit olarak görmüştür. İnternet ülke içindeki ticari faaliyetleri, bankacılık işlemlerini ve haberleşmeyi kolaylaştırmış, ABD'nin ekonomik kalkınmasına yardımcı olmuştur. Ancak kötüye kullanım her alanda olduğu gibi internet içinde de etkili olduğunu kısa sürede göstermiş ve bilgi güvenliğine ilişkin saldırılar görülmeye başlanmıştır.

Her ülkenin vatandaşlarını da kendine özgü bilgileri de internet ortamında koruması şarttır. Bunun içinde koruma yöntemlerini, hukuki kuralları ve yaptırımları içeren bir strateji geliştirmesi gerekmektedir. ABD, dijital önlemlerin yanı sıra, olası dijital saldırılara yönelik kapasitesini arttırmak için istihbarat ve güvenlik konusunda faaliyet gösteren kurumlarında, siber güvenlik birimleri kurmuştur. Elbette bunları yeterli görmemiş, özel sektörü güvenlik konusunda teşvik etmiş ve tamamen dijital güvenlik faaliyetlerine yoğunlaşan devlete ait yapılanmaları da hayata geçirmiştir [49].

3.1 Genel bakış

"ABD" ve "Siber Güvenlik" denildiğinde akla ilk gelen kurumlar kuşkusuz Federal Araştırma Bürosu (Federal Bureau of Investigation / FBI), ABD Merkezi Haber Alma Servisi (Central Intelligence Agency / CIA), ABD İç Güvenlik Bakanlığı (United States

Department of Homeland Security / DHS), Siber Komutanlık (CYBERCOM) ve Ulusal Güvenlik Ajansı (National Security Agency / NSA)'dır. Ülke için siber güvenlik yalnızca bilgi hırsızlığı endişesini değil aynı zamanda uzayla ilgili araştırmalar, devlet güvenliği, kişisel bilgilerin korunması ve devlet sırlarını da akla getirmektedir. Özellikle 2000 yılı sonrasında kalkınmış ülkeler arasında siber uzay kaynaklı teknolojik fırsatlara ilişkin ciddi rekabet söz konusu olmuştur. ABD dijital alanda güç kaybetmemek, liderliğine devam etmek ve güvenliğini sağlayabilmek için hem devlet hem de özel sektör eliyle sürekli gelişim stratejileri izlemeye başlamıştır [49].

ABD, siber saldırılar ve güvenlik konusunda dünyanın en güçlü ülkelerinden biridir. Fakat buna rağmen sürekli saldırılar ile karşılaşmaktadır. 2001 yılından bu yana devlet siber güvenlik konusuna sürekli gündeminde yer vermektedir. İlk defa George Bush döneminde, 2003 yılında "Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi" hazırlanmıştır. Bu stratejide federal hükümet, yerel yönetimler, özel sektör ve kamu gibi pek çok alanda odaklanılacak olan konular belirlenmiştir. Yayınlanan her stratejik planda amaçlar "Amerika'nın kritik altyapılarının siber saldırılara karşı korunması, siber saldırılara karşı ulusal hassasiyetin azaltılması ve saldırı sonrası zararın minimum seviyede tutulması" ekseninde şekillenmiştir. Ayrıca stratejinin beş adet kritik önceliği mevcuttur. Bunlar [44]:

i "Ulusal Siber Uzay Güvenlik Müdahale Sistemi,

ii Ulusal Siber Uzay Güvenlik Tehdit ve Zafiyet Azaltma Programı,

iii Ulusal Siber Uzay Güvenlik Farkındalık ve Eğitim Programı,

iv Kamu Siber Uzayının Korunması, Ulusal Güvenlik ve

v Uluslararası Siber Uzay Güvenlik İşbirliği" şeklindedir

3.2 Kamu-Özel Sektör İşbirlikleri ve Sorumlu Kurumlar

Önceki bölümlerde fark edildiği üzere, ABD siber güvenlik konusunda en fazla yatırımı yapan ve konuyla ilgili projeler ile kalifiye eleman üreten ülkeler arasındadır. Ülkenin, siber sistemlerinin geliştirilmesi, önlemlerin arttırılarak saldırılara karşı hazırlıklı olunması ve uzay teknolojilerinin arttırılarak üretim, savunma ve bilim alanlarında daha fazla güçlü olabilmesi için pek çok kurum ve kuruluş görev almaktadır. Bu kuruluşların

hangi olduğunu ve hangi görevleri yerine getirdiklerini, kurdukları ortaklıkları şu şekilde listelemek ve özetlemek mümkündür:

ABD Savunma Bakanlığı (United States Department of Defense) ve Siber Komutanlık (CYBERCOM) adından da anlaşılacağı üzere, ülkenin uluslararası alanda korunmasından sorumlu olan bakanlık, 1947 yılında faaliyetlerine başlamıştır. Bu kurum genelkurmay başkanlığı görevini de yürütmektedir. Kurum, askeri icraatların yanı sıra siber güvenlik hususunda da etkin göreve sahiptir. Kurum bünyesinde siber güvenlik faaliyetleri için kurulan STRATCOM'un alt birimi olan CYBERCOM, askeri bilgisayar ağlarının saldırılara ve arızalara karşı korunmasından sorumludur. Burası ayrıca siber kaynakların düzenlenmesi konusundan da sorumludur. CYBERCOM tüm bu görevlerinin yanı sıra, siber saldırganların yetiştirilmesinden de sorumludur. Bu savaşçıların bilinen sayısı 5000'den fazladır ve ABD'nin uluslararası alanda siber gücünün önemli bir parçası CYBERCOM, onun savaşçıları ve diğer siber güvenlik birimleridir [49].

i Federal Araştırma Bürosu (Federal Bureau of Investigation / FBI) Özünde Adalet Bakanlığı bünyesinde faaliyet gösteren FBI, ülke içinde işlenen suçların araştırılması konusunda görev almaktadır. İstihbarat yapma yetkisi olan kurum siber tehdit konularında da bu yetkisini kullanabilmektedir. Özellikle DHS, siber alanlarda bilgi desteğini FBI'dan almaktadır ve bu hususta iki kurum birlikte çalışmaktadırlar [42].

ii ABD İç Güvenlik Bakanlığı (United States Department of Homeland Security / DHS)

DHS'nın kurulması 11 Eylül olayının sonrasına rastlamaktadır. 2002 yılında hizmet vermeye başlayan bu kurumun amacı terör örgütlerinden kaynaklanan siber saldırıları önlemek ve devleti bunlar tarafından gelen risklere karşı korumaktır [42] [50].

Bu kurum siber güvenliğe ilişkin projelerin koordinasyonu görevini de üstlenmektedir. Kurumun kuruluş kanununda da İç Güvenlik Bakanlığı'nın gerekli hallerde diğer kurum ve kuruluşları birlikte hareket etmeye davet edebileceği belirtilmektedir. Hem ulusal hem de yerel yönetimlerde siber alanda tehdit oluşturabilecek unsurları tespit etmek ve bunlara müdahale etmek için bakanlığa ait alt kuruluşlar mevcuttur. Bu kuruluşlar yerel yönetimler ile iş birliği içindedirler. Bakanlığa bağlı Ulusal Siber Güvenlik ve iletişim Entegrasyon Merkezi (National Cyber Security and Communications Integration Center / NICIC), kamu kurum ve kuruluşlarıyla özel sektöre ait olan meselelerdeki güvenliği de uyumlu hale getirmektedir [49].

iv. ABD Merkezi Haber Alma Servisi (Central Intelligence Agency / CIA) CIA FBI ile benzer faaliyetler yürütmesine karşın faaliyet alanı ABD dışıdır. Bu gizli servis, ABD'yi tehdit edebilecek dış hareketler konusunda istihbarat sağlamaktadır. Kurum tarafından yürütülen tüm operasyonlar gibi siber alandaki operasyonları da gizli bilgi niteliğindedir. Ayrıca kurum kimi zaman gerekli gördüğü takdirde dışarıya da saldırı düzenleyebilmektedir. Örneğin Sovyet Sosyalist Cumhuriyetler Birliği Sibirya Gaz boru hattına yapılan ve adına mantık bombası denilen saldırıdan CIA'nin sorumlu olduğuna dair görüşler oldukça yaygındır [49].

v. Ulusal Güvenlik Ajansı (National Security Agency / NSA) NSA ABD için siber güvenlik alanında faaliyet gösteren diğer önemli bir kuruluştur. Kurumun hem çalışanları hem de bütçesi gizli tutulmaktadır [51]. Kurumun ana amacı kriptanalizdir. Hem ordu hem de diğer devlet kurumları için Merkezi Güvenlik Servisi (National Security Servise / CSS) ile ortaklaşa çalışarak bu hizmeti vermektedir. NSA'nın başkanı aynı zamanda CYBERCOM ve CSS'nin de şefi olarak görevlendirilmektedir. Bu sayede kurumlar arasında koordinasyon da garanti altına alınmış olmaktadır [52].

NSA'ya ilişkin bir iddia olan telefon, e-posta, internet izleme ve dinleme "Edward Snowden Olayı" ile gündeme gelmiştir. Olayla ilişkili telefon sesleri ve e-posta kayıtlarının NSA'ya ait olduğuna ilişkin haberler basında yer almıştır. Hatta o dönemde kurumun yetkisi olmamasına karşın sivilleri de gözlediğine ilişkin görüşler yüksek sesle söylenmeye başlanmıştır [49].

Tüm bu kurumların bağlı oldukları ve siber güvenlik sistemlerinin koordine edildiği ana kuruluş ABD Savunma Bakanlığı (United States Department of Defense)'dır. Ancak bu bakanlık İç Güvenlik Bakanlığı ve Federal Araştırma Bürosu ile iş bölümü yapmıştır [50]. Bu kurumların temsil edildiği, ortak olarak çalıştıkları Ulusal Güvenlik Konseyi (National Security Council / NSC) ülkenin siber alandaki politikalarını belirlemektedir ve diğer kurum ve kuruluşlar ile bunların ortaklıklar ile yürüttükleri projeler bu politikalara uyumlu olarak gerçekleştirilmektedir. Ayrıca yukarıda sayılan kurumlar dışında, Hükümetin siber güvenlik konuları ve hükümet tarafından politikaların uygulanmasını ise Bilgi ve İletişim Altyapıları Kurumlar Arası Politika Komitesi (Information and Communications Infrastructure Interagency Policy Com-mittee / ICI-IPC) yürütmektedir. Bununla birlikte CSS, ülke çapındaki siber güvenlikle ilişkili tüm çalışmaların entegre biçimde yürütülmesinin ve bu faaliyetlerin gözetlenmesinin de sorumluluğunu yerine getirmektedir. Kurumların

koordinasyonu ve politikaları hayata geçirmeleri konusunda destek sağlayan bir diğer bakanlık ABD Adalet Bakanlığı (The Department of Justice/DoJ)'dur. Tüm bunların yanı sıra çeşitli bakanlıklara ve sivil topluma bağlı olan çeşitli kuruluş mevcuttur [49].

3.3 Eğitim ve Farkındalık Çalışmaları

Siber alanda güvenliğin sağlanması yalnızca kötü yazılımları ayırt ve takip eden programlar ve yasal düzenlemeler ile mümkün değildir. Kullanıcıların, yasa yapıcıların, sistem yöneticilerinin ve şirket sahiplerinin siber teknolojiler ve bilgi hırsızlığı riskleri konusunda eğitimli olmaları şarttır. Bu nedenle güvenlik konusundaki stratejilerin içinde eğitim ve bilinçlendirme çalışmalarına da yer verilmesi gerekmektedir. Eğitim ve farkındalığa ilişkin ABD siber güvenlik stratejisinin 4 temel odak noktası bulunmaktadır. Bunları şu şekilde sıralamak mümkündür [44]:

i Tüm ABD'de halkın ulusal güvenlik, bireysel güvenlik ve siber uzayı konusunda bilgi sahibi olmasına imkan yaratacak programlar oluşturmak ve ulusal bir farkındalık programı kapsamında buna ilişkin faaliyetler yürütmek; kişinin kendisi ve ulusu için güvenlik konusunda eğitim alması, interneti ve internet ile bağlantılı cihazları tanıması gerekmektedir. Bu sayede, kendi cihazlarında bile erişim izinleri konusunda daha dikkatli davranacak, ev ve işyerlerinde önlem almak için yardım arayışına girmeleri bile hem konuya ilişkin ekonomik faaliyetleri arttırmakta ve riskleri düşürmektedir.

ii Ulusal siber güvenlik için halkın da katılım sağlayacağı eğitim programları gerçekleştirmek; özellikle gençleri siber güvenlik konusunda eğiterek onların kendi projelerini oluşturması için olanak sağlamak mümkündür. Yeni fikirler, yeni savunma yöntemleri anlamına gelmektedir.

iii Var olan siber güvenlik ile ilgili eğitim programlarının etkinliğini arttırmak; bu sayede genç neslin siber güvenlik konusunda bilinçliliği artacaktır. Güvenlik alanında faaliyet gösteren kurumlara da çalışan yetiştirmek ve gençlerin bu alanda meslek seçmeleri için onlara konuyu sevdirmek adına eğitimler daha etkin hale getirilmelidir.

iv Kamu-özel sektör iş birliğini profesyonel siber güvenlik sertifikasyonları için desteklemek hem kamu kurumlarının hem de özel sektörün birlikte projeler yapması ve onların projeler esnasında güvenliğe ilişkin standartlara uyması riskleri düşürecektir.

ABD, halkın interneti en yaygın kullandığı ülkelerden biridir. Bu nedenle bilinçli kullanım konusunda farkındalığın arttırılması çok önemlidir. Medyada da konuya ilişkin reklamlar yayınlanmaktadır. Ayrıca güvenlik konusunda mobil aplikasyonlarda hangi izinlere dikkat edilmesi konusunda halk bilinçlendirilmeye çalışılmaktadır. ABD literatürü de siber güvenlik konusunda oldukça zengindir ve bu sayede üniversiteler başta olmak üzere, çeşitli sektörlerdeki işverenler ve teknoloji geliştiricilerinin farkındalıkları artmaktadır [53].

Güvenliğe ilişkin eğitim çalışmalarını yürütmek üzere, Amerikan Eğitim Bakanlığı pek çok kurumun da desteği ile Ulusal Siber Güvenlik Eğitim Girişimi (National Initiative for Cybersecurity Education,NICE)'ni başlatmıştır. Bu programın amacı var olan güvenlik sistemlerine ilişkin bilgiyi arttırmak ve her yaştan bireye konu ile ilişkili farkındalığı aşılamaktır. Ayrıca NICE okullardaki fen ve teknolojiyle ilgili derslere program hazırlamakta ve ders programına konuyu entegre etme amacı taşımaktadır. Ulusal Akademik Mükemmeliyet Merkezleri'nde ise ülke içinde siber Güvenliğe ilişkin yükseköğrenim düzeyinde mesleki eğitim verilmektedir [44] [54] [55].

Bölüm 4

Avrupa Birliği'nin Siber Güvenlik Stratejisinin İncelenmesi

4.1 Genel bakış

Avrupa Birliği'nin siber güvenlik konusundaki ilk stratejik adımları 2004 yılında atılmaya başlanmıştır. AB komisyonu, bu tarihte siber güvenlik konusunu kişi ve ulusun birimlerine zarar verecek, üye hükümetlerin etkin ve verimli ekonomik refahı üzerine negatif etki yapacak, terör riski oluşturacak her türlü teknolojiyi tehdit olarak ele almıştır. Aynı şekilde bu dönemde güvenlik ve teknoloji konuları ile ilgilenen birimlerin altyapılarının ne olduğu, nasıl oluşturulması gerektiği ve korunma konusunda neler yapılabilmesine ilişkin ilk defa tanımlamalar yapılmıştır. Komisyon, finans merkezleri ve finans ile ilgili bilgi barındıran birimleri, iletişim ve bilgi teknolojisi konusunda faaliyet gösteren şirket ve kamu kuruluşlarını, enerji tesislerini ve iletişim ağlarını korunması gereken en önemli merkezler olarak seçmiştir. Ayrıca temiz ve güvenilir gıdaya ulaşım, enerji üretimi ve toplu ulaşım ağlarını da önemli olarak işaretlemiş ve buraların güvenliğe ilişkin altyapılarının düzenlenmesini, gerekli önlemlerin alınmasını istemiştir [42].

Avrupa Birliği'nde ABD ve diğer ülkelere yapılan büyük siber saldırılar panik yarattığından, 2005 yılında Yeşil Kitap yayınlanmıştır. Yeşil Kitap, siber güvenlik konusundaki eylem planlarını içeren bir belgedir. Bu planda, siber saldırı risklerinin en az düzeye indirilmesi için neler yapılması gerektiğine ilişkin bilgiler paylaşılmış ve olası saldırılarda ne tür hasarların oluşabileceğine dair tahminler yürütülmüştür. Kritik Altyapı Erken Uyarı

Bilgi Ağı (Critical Infrastructure Warning Information Network) da aynı dönemde hayata geçirilmiştir. 2010 yılında AB Komisyonu, "Dijital Gündem"i hayata geçirmiştir. Bu adımda amaç ağ ve bilgi güvenliğini sağlamak ve olası riskleri tespit ederek bunlar için önlem almaktır [56].

2010 yılı Lizbon'da AB ve NATO'nun ulusal güvenliğe ilişkin daha fazla düzenleme yapılması gerektiğine karar verilen yıl olmuştur. Bu toplantıda siber güvenlik ile ilgili bir merkez kurulması gerektiğine de karar verilmiştir. Bunun neticesinde Avrupa Siber suç Merkezi (EC3- European Cybercrime Centre) ve Bilgisayar Acil Müdahale Ekibi (CERT-Computer Emergency Readiness Team) kurulmuştur [44].

AB'deki siber güvenliğe ilişkin politikalar 2016 yılında revize edilmiştir [57]. Bu düzenlemeler ile 2010 yılında yetkilendirilen ENISA (European Union Agency For Network and Information Technology)'nın da yetkileri arttırılmıştır. ENISA yalnızca AB'de değil küresel düzeyde siber güvenliğe ilişkin önlemlerin alınması için ABD ve diğer ülkeler ile birlikte projeler yürütmektedir.

4.2 Eğitim ve Farkındalık Çalışmaları

AB'nin siber güvenlik konusundaki en önemli önceliklerinden biri eğitimdir. Çocuk ve gençlerin bilgisayar kullanımlarının çok yoğun olması, konu hakkındaki eğitim konusunda onlara öncelik verilmesini gerekli kılmıştır. Eğitim kurumları, gençlerin siber dünya konusu ile ilgili bilinçlendirilmesi konusunda paydaşlar arasına alınmış okul müfredatlarına kademeli olarak siber güvenlik konularının yerleştirilmesine karar verilmiştir. Eğitime yönelik AB içinde yapılan çalışmaların odak noktasındaki konuları şu şekilde sıralamak mümkündür [42] [58]:

i Öncelikle hangi kitlelerde konuya ilişkin bilinçlilik oluşturulacağına karar verilmelidir. Kimlerin interneti hangi sürelerde ve hangi maksatlarda kullandıkları tespit edilmeli, özellikle genç ve çocuklara onlara eğlenceli gelecek şekilde konu açıklanmalı ve bireysel olarak neler yapabilecekleri öğretilmelidir.

ii İnternet kullanımı gerçekleştiren bireylere hangi yollar ile ulaşılacağı belirlenmelidir.

iii Gençlerin internet alanında hatalı davranışlarının neler olduğu izlenmeli, okullarda bu davranışların dönüştürülmesi için programlar oluşturulmalıdır.

iv Çok bilinen kamu sitelerine bilgi güvenliği ile ilgili sunum, materyal, dersler konulmalı, bu sayede gençlerin ve halkın göz aşinalığı oluşturulmalı, siber güvenlik konusunda merak uyandırılmalıdır.

v Her ülkede siber güvenlik konusundaki bilgi ve belgeler ana dillere çevrilmeli, herkesin anlayabileceği şekilde konunun sunumu yapılmalıdır.

vi Müfredata mutlaka internet ve güvenlik konuları eklenmeli, özellikle üniversitelerde bilinçlendirme çalışmaları arttırılmalıdır.

vii Siber güvenliğe ilişkin mesleki eğitimler verilmelidir.

viii Kritik görevler için gençler isteklendirilmeli, siber güvenliğe ilişkin üniversite bölümleri açılmalı, sertifika programları oluşturulmalıdır. Ayrıca tüm programların uluslararası akreditasyonları olması için uyması gereken standartlar belirlenmelidir.

Avrupa'da internet üzerinde kişilerin korunabilmesi için yapılan bir diğer farkındalık çalışması ise, onları kişisel verileri korumanın bir insanlık hakkı olduğu yönünde eğitmektir. Her kurum kişisel verileri isterken –internet ortamı dahil- kişisel verilere ilişkin güvence vermekte, işlenme ve saklama konularında izin istemektedir. Bu sayede kişisel verilerin başkalarının eline geçmesi halinde neler olabileceğine dair de bir farkındalık oluşturulmuş olmaktadır [59].

4.2.1 European Cyber Security Month

European Cyber Security Month (ECSM) vatandaşların ve kurumların bilgi güvenliğinin önemi hakkında siber güvenliği teşvik eden kişisel, finansal ve kurumsal verilerin korunması için yapılması gerekenleri vurgulayan Avrupa Birliği bilinçlendirme kampanyasıdır. Kampanyanın amacı farkındalığı arttırmak, kişi ve kurumların kendilerini çevrimiçi risklerden nasıl koruyabilecekleri konusunda kaynak sağlamaktır. The European Union Agency for Network (ENISA), European Commission DG Connect and Partners her 5 yılda bir Ekim ayında olmak üzere ECSM'yi görevlendirmektedirler [54]. ECSM hedef kitlesi genel halkı içermekle birlikte, "AB Dijital Vatandaşları "olarak hareket etmek ve üye devletlerin kamu ve özel kuruluşlarından paydaşlara odaklı belli grupları kapsamaktadır.

ECSM'nin hedeflerini şu şekilde sıralamak mümkündür;

i AB Siber Güvenlik Stratejisinde belirlenen önceliklerden bir tanesi olan siber güvenlik konusunda farkındalık yaratmak.

ii İnternetin daha güvenli kullanımı için tüm kullanıcıları teşvik etmek.

iii Siyasi ve medya koordinasyonu yoluyla bilgi güvenliğine yönelik ilgiyi arttırmak.

iv Projenin Avrupa ve küresel boyutu aracılığıyla ulusal medyanın ilgisini çekmek.

4.2.2 Kritik Altyapı Uyarı Bilgi Ağı (CIWIN)

AB içinde, ulusların halklarının ve yönetimlerinin bilgi güvenliğine ilişkin farkındalıklarını arttırmaları üzerine faaliyet gösteren bir diğer kampanya da Kritik Altyapı Uyarı Bilgi Ağı (CIWIN)'dir. AB komisyonu tarafından oluşturulan bu sistem, riskler ve güvenlik tehditleri konusunda uyarı verme amacına hizmet etmektedir. CIWIN, devlet kurumları ve özel işletmeleri uyarmanın yanı sıra buraların tehditler karşısında neler yapabileceğine dair danışmanlık hizmetinde de bulunmaktadır [60].

4.3 Kamu-Özel Sektör İşbirlikleri ve Sorumlu Kurumlar

ENISA AB içinde siber güvenlik konusunda en fazla farkındalık sağlayan kuruluşlar arasındadır. Kendi eğitim programlarının yanı sıra web sitesi üzerinde kişilerin siber güvenlik konusundaki bilgilerini ölçmeleri için çeşitli testler düzenlemekte; eksikliklere göre bulabileceği dokümanlar sunmaktadır [58].

Farkındalığa ilişkin atılan en önemli adımlardan biri de siber güvenlik konusunda kurum ve kuruluşların bilinçliliğinin yükseltilmesi yönündedir. Siber güvenliğin sağlanması için öncelikle kurumlarda şeffaf bir yönetim anlayışının belirlenmesinin şart olduğuna karar verilmiş ve kuruluşları denetleyen mekanizmaların güçlendirilmesi ve yaptırımlar hakkında da halkın bildirilmesi gerektiği belirtilmiştir. Ayrıca AB'de halkın konu ile ilgili bilgilendirilmesi için sivil toplum kuruluşlarından da yardım alınması amacını taşıyan çalışmalar başlatılmış, her sivil toplum kurumu ile iletişime geçilmeye başlanmıştır. Bu kuruluşlar halkı kendilerine ait bilgileri paylaşırken nelere dikkat etmeleri konusunda uyarmakla görevlendirilmiştir. Teknoloji konusunda faaliyet gösteren sivil toplum kuruluşları kitapçıklar ve atölye çalışmaları yapmaya başlamışlardır [42] [54].

Kuşkusuz hemen her alanda olduğu gibi, AB'nin siber güvenliği konusunda da mevzuat ve standart oluşturan en önemli kurum, AB Konseyi'dir. Konsey'in aldığı şu kararların tamamı siber güvenlik ile ilişkilidir [60]:

i. 24 Şubat 2005 tarihli Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı

ii. 2006 tarihli Verilerin Saklanması Direktifi (2006 24 AT)

iii. 2002 tarihli Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi (2002 58 AT)

iv. 1995 tarihli Verilerin Korunması Direktifi (95 46 AT)

Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), uluslararası özellikle AB alanda bilgi sızıntılarının engellenmesi, siber suçların önüne geçilmesi ve ülkelerin iş birlikleri, politikaları, ekonomik kararları, ticari verileri gibi çeşitli önemli bilgilerinin güvende tutulması için önlemler alan ve projeler üreterek önerilerde bulunan bir diğer oluşumdur. OECD kritik bilgi altyapılarının, bilgi sistemlerinin ve şebekelerin güvenliği konularında uzun yıllardır yol gösterici çalışmalar yapmaktadır. Kuruluşun Bilgi Güvenliği ve Gizlilik Çalışma Grubu (WPISP), dünya genelinde ülkeleri siber suçlar ve kötü amaçlı yazılımlar konusunda uyarmakta; ülkeleri siber güvenlik politikası oluşturmak konusunda isteklendirmektedir. Ayrıca oluşuma ait Bilgi, Bilgisayar ve Haberleşme Politikaları Komitesi (ICCP) mevcuttur.

Bölüm 5

Türkiye'nin 2016 – 2019 Siber Güvenlik Stratejisinin İncelenmesi

5.1 Genel Bakış

Türkiye'de eğitim konusu sürekli olarak gündemde olan, stratejileri değişen ve buna karşın her zaman eleştirilen bir konu olmuştur. Eğitim, çeşitli konularda kişilerin bilinçlilik ve bilgi düzeylerini arttırmak olarak tanımlanabilecektir [61] ve toplumun ihtiyaçlarına göre planlanmalıdır. Siber güvenlik de çağın en önemli sorunlarından biridir ve hem bireysel hem de örgütsel düzeyde buna ilişkin bilginin ve deneyimin arttırılması şarttır.

Bu nedenle siber güvenliğe ilişkin hazırlanan 2006-2010 Eylem Planı uyarınca, TÜBİTAK 2007 yılından itibaren, 4 farklı kamu kurumu için Bilgi Güvenliği Yönetim Sistemini oluşturmuştur. Ayrıca değişik etkinlikler düzenleyerek kamu kurumlarının ve hatta özel sektör kuruluşlarının bilgi güvenliği konusundaki bilinçlilik düzeyini arttırma çalışmalarına başlamıştır. Bunun yanı sıra, TÜBİTAK Siber Olaylara Müdahale Ekipleri (SOME) arasında tatbikatların düzenlenerek olası bir saldırı karşısında deneyim elde edilmesine öncülük etmiştir. Bilişim Teknolojileri Enstitüsü (BTE), Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) kurularak sonrasında bunlar aynı çatı altında birleştirilmişlerdir. Kurumlar eğitim ve farkındalık çalışmalarına eğilmişlerdir. TÜBİTAK BİLGEM'de Yazılım Teknolojileri Araştırma Enstitüsü (YTE), Siber Güvenlik Enstitüsü (SGE) ve İleri Teknoloji Araştırma Enstitüsü olmak üzere üç yeni enstitü kurmuştur [62]. Ancak elbette bu yeterli değildir. Ana problem gençlerin ve halkın gündelik yaşamda konu

hakkında bilinçlendirmesi için yeterli kurum ve programın olmamasıdır. Özellikle AB ve ABD ile kıyaslandığında Türk eğitim sisteminin konu ile ilgili girişimlerinin oldukça dar olduğu fark edilecektir.

Türkiye'de Siber Güvenlik çalışmaları kapsamında Siber Güvenlik Kurulunun oluşturulması, 11 Haziran 2012 tarihinde 2012/3842 sayılı Bakanlar Kurulunca alınan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin karar ile 28447 sayılı 20/10/2012 tarihli Resmî Gazetede yayınlanarak yürürlüğe girmiştir. Alınan karara istinaden Türkiye için oluşturulan Siber Güvenlik Kurulu'nun yanı sıra, konuya ilişkin yetki ve görevler Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na verilmiştir. Ayrıca, siber güvenlik ile alakalı çalışma grupları ve geçici kurulların gerekli hallerde oluşturulması yönünde de karar verilmiştir.

Alınan bu bakanlar kurulu kararının içeriğine 06/02/2014 tarihinde yayımlanan 6518 saylı kanun ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen Ek Madde 1 ile kanunlaştırılmış, 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen ek fıkralar ile Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili yeni görevler verilmiştir.

Siber Güvenlik Kurulu, 5809 sayılı Elektronik ve Haberleşme Yasası'nın 1. Maddesinde düzenleme yapılmıştır. Madde 1'de ki düzenlemeye göre, Siber güvenlikle ile alakalı olarak gerçek ve tüzel kişilerle kamu kurum ve kuruluşlarının alacağı tedbirleri tayin etmek, hazırlanan program, usul, esas, rapor, plan ve standartları onaylamak, uygulanmasını ve koordinasyonunu sağlamak maksadıyla, UDHB Bakanının başkanlığında Siber Güvenlik Kurulu kurulmuştur. Siber Güvenlik Kurulunda bulunacak olan bakanlık ve kamu kurum ve kuruluşları ile bu bakanlıkların üyelerinin temsil seviyesi Bakanlar Kurulunca belirlenmektedir.

Kurulun görevleri,

- Siber güvenlik ve bununla ilişkili olan durumlar hakkında oluşturulan politikaların, stratejilerin ve eylemlere ilişkin planların onaylanmasıyla birlikte ülke genelinde etkili biçimde uygulanabilmesi için gereken kararların alınması,
- Kritik altyapıların belirlenmesi ile alakalı teklifler için kararların verilmesini sağlamak

- Siber güvenlikle alakalı kararların uygulanması esnasında özel sebepler ile istisna olan kurumların hangileri olduğunu belirlemek
- Kanunlarla verilen diğer görevleri yerine getirmek.

Olarak belirlenmiştir.

"Siber Güvenlik Kurulunun çalışma usul ve esasları Başbakanlıkça çıkartılacak yönetmelikle belirlenir."

5809 sayılı Elektronik ve Haberleşme Kanununa eklenen Ek Madde 1 de oluşturulacak olan Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafında belirlenir ifadesi yer almaktadır. [63] Kanunun referans gösterdiği 2012/3842 sayılı 11 Haziran 2012 tarihli Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu kararları gereğince Siber Güvenlik Kurulu Ulaştırma, Denizcilik ve Haberleşme Bakanı Başkanlığında, Dışişleri Bakanlığı Müsteşarı, İçişleri Bakanlığı Müsteşarı, Milli Savunma Bakanlığı Müsteşarı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı[1] İle UDHB Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmaktadır.

Siber Güvenlik Kurulu, 21 Aralık 2012 tarihinde UDHB Bakanı başkanlığında toplanmış ve aldığı kararlar içerisinde "Ulusal Siber Güvenlik Stratejisi ve 2013 – 2014 Eylem Planı" kabul görmüştür [64].

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın kabulü; Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 18 Ocak 2013 tarihli ve 412 sayılı yazısının ardından, Bakanlar Kurulu tarafından 25 Mart 2013'te kararlaştırılmış, sonrasında 20 Haziran 2013 tarihli 2013/4890 karar ile 28683 sayılı Resmi Gazetede yayımlanmıştır [65].

[1] 17 Ağustos 2016 tarihinde Resmi Gazetede yayımlanan 671 sayılı KHK ile Telekomünikasyon İletişim Başkanlığı kapatılmıştır. http://www.resmigazete.gov.tr/eskiler/2016/08/20160817-18..htm

Şekil 5.1: Ulusal siber güvenlik organizasyonu.

Artan güvenlik gereksinimleri ile gelişen bilgi ve iletişim teknolojileri doğrultusunda da UDHB'nin ulusal siber güvenlik stratejisini güncellemesinin yanı sıra 2016 -2019 yıllarını içine alan faaliyetlere karar vermesi ihtiyacı meydana gelmiştir. Öncelikli olarak 2013 – 2014 eylem planında yer alan kurumlar ile 10 Mart – 7 Nisan 2015 aralığında 7 tane değerlendirme toplantısı yapılmış, eski eylem planında bulunan faaliyetlerin gerçekleşme oranları ile yaşanan zorluklar ve bununla birlikte gelecek konusundaki değerlendirmeler ile siber güvenlik özelinde gerçekleştirilmesi gerekli olan uygulamalar da ayrıntılı biçimde belirlenmiştir.

Toplantının akabinde kamu kurum ve kuruluşları, kritik altyapı işletmecileri, üniversiteler, sivil toplum kuruluşları ve bilişim sektörünü temsil edecek şekilde 73 farklı kurum ve kuruluştan toplamda 126 uzman personelin katılımıyla Ortak Akıl Platformu gerçekleştirilirmiştir. Platform çalışması iki gün sürmüş ve Türkiye'nin siber güvenlik alanında güçlü ve zayıf yönlerinden yola çıkılarak stratejik hedeflerin yanı sıra gerçekleştirmesi gereken faaliyetler tespit edilmiştir.

2008 yılından itibaren Ekonomik İş Birliği ve Kalkınma Teşkilatı (OECD), Kuzey Atlantik İttifakı (NATO), Avrupa Birliği (AB) gibi uluslararası kuruluşların dışında diğer gelişmiş ülkelerin de gündemine girmiş durumdadır. 2016 -2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanırken paydaşlarla birlikte yapılan çalışmalara ek olarak, Avrupa, Amerika ve Uzak Doğu'dan çok sayıda ülkenin de siber güvenlik stratejileri

incelenmiştir. Siber güvenlik alanında kapsam, hedefler, organizasyon yapıları, kamu özel sektör iş birlikleri, Ar- Ge çalışmaları, eğitim gibi alanlarda üretmeye çalıştıkları çözümler detaylı olarak incelenmiştir.

Tüm bu çalışmaların çıktısı sonucunda da halen yürürlükte olan 2016 – 2019 Ulusal Siber Güvenlik Stratejisi ve 2016 – 2019 Ulusal Siber Güvenlik Eylem Planı hazırlanmıştır [12].

Eğitim ve farkındalık stratejileri, 2013 – 2014 Ulusal Siber Güvenlik Eylem planının içerisinde siber güvenlik riskleri başlığı altında siber güvenlik hususunda kurumsal ve kişisel seviyede yeterli bilgi ve bilinç seviyesine ulaşılamaması risk olarak tanımlanmıştır.

Siber güvenlik alanında insan kaynaklarının oluşturulması ve arttırılmasının yanında, konuyla alakalı bilinçlendirme faaliyetleri başlığı altında orta ve uzun vadede siber güvenlik alanında insan kaynağının üretilmesine yönelik çalışmaların arttırılacağı ve hız kazanacağı belirtilmiştir. İlkokul döneminden üniversiteye kadar tüm eğitim programlarında siber güvenlik kavramının yer edinmesine yönelik eğitim programlarının oluşturulacağı ve ders içerikleri hakkında şekillendirmeler yapılacağı belirtilmiştir. Ancak yalnızca okullarda gerçekleştirilecek olan bu eğitim yenilemesi elbette yeterli olmayacağından, siber güvenlik konusunda genel bir bilgi sahipliğinin sağlanması için halka yönelik bir eğitim platformunun kurulacağı ve bu eyleme hizmet etmek amacıyla ortaya çıkan girişimlerin destekleneceği eylem planında yer almıştır. Bu kapsamda meslek liselerinin bilgisayar programcılığı bölümlerindeki müfredata siber güvenlik eklenmesi, Fatih projesi içeriğine siber güvenlik konulu eğitimlerin eklenmesi, bilişim teknolojileri alanında verilen kurs programlarının arasına siber güvenlik eğitimlerinin dahil edilmesi alt eylem olarak belirtilmiştir. MEB sorumlu olmak üzere, TUBITAK ve BTK ilgili kurumlar olarak Mart 2014 tarihinde bitirilmesi belirtilmiştir.

2013 – 2014 Ulusal Siber Güvenlik Eylem Planı içinde bilgisayar kullanıcılarının siber güvenlik konusunda bilinçlendirilmesine yönelik eylemin alt eyleminde, bilgisayar kullanıcılarının siber güvenlik konusunda bilinçlenmesinin arttırılmasına yönelik eğitim faaliyetleri, seminerler, broşürler, uzaktan eğitim programları gibi çalışmalar yapılması ve güvenli internet kullanımı konusunda da bilinç düzeyinin arttırılması ve bu hizmetlerin geliştirilmesi ve yaygınlaştırılması ifade edilmiştir. Bu madde için ise BTK sorumlu, MEB, UDHB ve RTÜK ilgili kurumlar olarak belirtilmiştir.

2016 – 2019 Ulusal Siber Güvenlik Stratejisi içerisinde ise Stratejik Siber Güvenlik Amaçları ve Eylemleri başlığı altında yer alan sekizinci madde de "Toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması." olarak yer almaktadır.

5.2 Eğitim ve Farkındalık Çalışmaları

Türkiye'de eğitim programlarından sorumlu olan bakanlık Milli Eğitim Bakanlığıdır. Ulusal Siber Güvenlik Sistemi programında da eğitim alanında konuya ilişkin yapılacak olan düzenlemeler 22. maddede düzenlenmiştir. Buna göre [42];

i Özellikle konuyla ilgili ara eleman yetiştiren meslek liselerinde, bilgisayar programcılığı bölümlerinin ders programlarına siber güvenliğe ilişkin konular yerleştirilmelidir.

ii Bilişim teknolojileri bünyesindeki kurs programlarına siber güvenlik konusu için de yer açılması gereklidir. Halkın eğitilmesi için devlet tarafından da çeşitli kursların açılması gerekmektedir.

iii Fırsatları Arttırma ve Teknolojiyi İyileştirme Hareketi (FATİH) Projesi oluşturulmuş ve bu proje kapsamına siber güvenlik konusu dahil edilmiştir.

iv Bilgi teknoloji eğitimleri için açık kaynak kodlu ürünler yer almaya başlamalıdır.

Elbette eğitim alanında yapılan düzenlemeler siber güvenliğin sağlanması için yeterli değildir. Halkın tamamının buna katılması ve konu hakkında bilinçlenmesi şarttır. Bu nedenle farkındalık çalışmalarına da önem verilmelidir.

Farkındalık halkın bir konu hakkında bilinçlenmesini sağlamaktır. Türkiye'de siber güvenlik konusunda bilinçlendirmek için öncelikle eğitim alanında müfredatta bu konulara değinmek gerektiğine karar verilmiş, tabletler dağıtılarak çocuklara internet kullanımı konusunda bilgi verilmeye başlanmıştır [2]. Gençlerin bu sayede internet ile kontrollü biçimde tanışması amaçlanmıştır. Ayrıca interaktif bir öğrenme ortamının oluşturulması hedeflenmiştir [66].

[2]Fatih projesi kapsamında dağıtılan tabletlerin yeterli derecede eğitimi desteklemediği, kolay kırıldığı ve ihalelerin süreçlerinin uzaması gibi sebepler ile bunun dağıtımı 2018 yılında durdurulmuş, Bakanlık klavyeli masaüstü bilgisayarların dağıtılacağını açıklamıştır. Bkz: Cumhuryet Gazetesi 05 Şubat 2018 tarihli haber: http://www.cumhuriyet.com.tr/haber/egitim/920594/Tablet_yok..._Fatih_Projesi_de_coktu.html

Bunun yanı sıra çalışanların özlük hakları ile ilgili düzenlemelere siber güvenliğe ilişkin maddelerin yerleştirilmesine karar verilmiştir. Bu sayede çalışırken kişilerin konu hakkındaki bilinçliliği artacak ve aynı zamanda iş yerlerinde siber saldırılara ve bilgi sızıntılarına karşı daha dikkatli davranabileceklerdir. İş dünyasında çalışanların bilinçlendirilmesi, halkın doğrudan ve dolaylı olarak bilinçlendirilmesi anlamına gelmektedir. Siber güvenlik alanında çalışanların yanı sıra öğrenci ve öğretmenlerin de konuya dikkatlerinin çekilmesi için kursların ve proje yarışmalarının düzenlenmesi gerekmektedir. Özellikle kodlama konusuna önem verilmeye başlanmıştır ve ulusal ve uluslararası yarışmalara katılması için gençler ve aileleri teşvik edilmeye başlanmıştır. Yeni eğitim sistemleri ve kurslar her kurumda, onların güvenlik stratejilerini oluşturacak personelin istihdam edilmesi için de ortam yaratılmış olmaktadır [12].

Türkiye'de halkın güvenli internet kullanımı ve siber güvenlik konusunda farkındalığının oluşturulması konusunda kamu spotlarından da faydalanılmaktadır. Radyo ve Televizyon Üst Kurulu (RTÜK) web sitesinde, yayınlanan kamu spotları listesine göre, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından "kablosuz internet kullanımı konusunda kamuoyunu bilinçlendirmek hakkında" kamu spotu hazırlanmıştır ve 13 Eylül 2018 tarihine kadar bu spot yayında kalacaktır. 2018'in 8.ayına kadar Kızılay ve Türkiye Cemiyeti tarafından hazırlanan "teknoloji bağımlılığı hakkında" ve Milli Eğitim Bakanlığı Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü tarafından hazırlanan "çocukların bilgisayarı sadece bir oyun ve eğlence aracı olarak görmemesi, bilgisayar karşısında tüketici olmaktan çıkıp üretici konumuna gelmeleri, karşılaştıkları sorunlara pratik çözümler üretebilmeleri, algoritmik düşünme becerilerini geliştirmeleri hakkında" kamu spotları yayında kalacaktır. "e-Devlet Kapısı hizmetlerinin kullanıcı sayısını artırmak, mevcut kullanıcıların farkındalığını yükseltmek, yaygınlık ve erişimi artırmak" ve "Sanayinin Dijital Dönüşümünde Yazılım ve Eğitimin Yeri" temalı sanayinin ihtiyaç duyduğu iş gücünü yetiştirmek, organize sanayi bölgelerinde mesleki ve teknik eğitim veren Anadolu lisesi (teknik kolej) açılmasını desteklemek", farkındalık hususunda yayınlanan diğer kamu spotlarıdır [67].

Görüldüğü üzere, Türkiye'de eğitime ve farkındalığa ilişkin çeşitli girişimler olsa da, bunlar yeterli düzeyde değildir. Hem kurumlar hem de yapılan eğitim ve farkındalık arttırma faaliyetleri AB ülkelerinin ve ABD'nin çok gerisindedir. Özellikle genç ve çocuklar, ancak bilgisayar ile ilişkili bölümlerde okuyorlarsa siber güvenliğe ilişkin bilgi edinebilmektedirler. Ancak tüm nüfusun bilgisayar ile kimi zaman seyrek de olsa bir teması mevcuttur.

Özellikle orta ve yüksek gelir düzeyindeki ailelerde çocuklar henüz okuma yazma öğrenmeden elektronik sistemler ile tanışmaktadırlar. Bu nedenle çok küçük yaşlardan itibaren çocuklara internetin ne olduğu, burada ne tür risk ve tehlikeler ile karşılaşabilecekleri, kendilerini bilgi kirliliği ve hırsızlığından nasıl koruyacakları konusunda eğitimler verilmelidir. Eğitimlerin çocukların dikkatlerini çekecek şekilde oyunlarla desteklenmesi ve yaş ile teknolojinin ilerlemesine göre sıklıkla yenilenen programların oluşturulması önemlidir. Bu çalışma, bu konuya dikkat çekebilmek adına, çocuklar arasında kısa bir eğitim çalışmasının bile etkilerinin olabileceğini gösterme amacını taşımaktadır ve Türkiye'nin siber güvenliğe ilişkin eğitim ve bilinçlendirme konusunda daha fazla efor sarf etmesi gerektiğine dikkat çekmektedir.

5.3 Karşılaştırma

Ülkelerin hemen her politikasında olduğu gibi, siber güvenlik sistemlerinde de uluslararası rehber kurumların tavsiye kararlarından ve birbirlerinden etkilendikleri unutulmamalıdır. ABD güçlü siber güvenlik sistemleri, AB ise üyeliğe kabul edilmek istenmesi, coğrafi yakınlık ve ortaklaşa yürütülen iş birlikleri gibi nedenler ile Türkiye'nin siber güvenlik politikaları üzerinde önemlidir. Tablo 5.1'deki çalışmada yapılan güvenlik politikaları araştırmaları neticesinde derlenmiştir:

5.4 Farkındalığı Arttıracak Kitlelerin Tespit Edilmesi

Siber güvenliğin sağlanması için bilgi güvenliği prensiplerinin yerine getirilmesi gerekmektedir ki ilk prensip kimlerin bilgi erişimi için yetkili olduğunun belirlenmesidir. Bir bilgi söz konusu olduğunda onun halka açık ya da bazı gurup veya kişiler arasında paylaşılacağının netleştirilmesi şarttır. Elbette kimlerin bilgiye erişeceğini belirlemek kimlerin önlem alması gerektiğini belirlemek için de önem taşımaktadır. Bilgiye erişim yetkisi olan kişilerin, onu değiştirme, saklama, yayma ve yok etme gibi konularda bilgi sahibi olması gereklidir. Aksi takdirde, bilginin güvenliğinden de emin olmak mümkün olmayacaktır [18].

Tablo 5.1: ABD, AB ve Türkiye Siber güvenlik politikaları eğitim ve farkındalık çalışmalarının karşılaştırması.

Değişkenler	Ülkeler		
	Avrupa Birliği	ABD	Türkiye
Eğitim Çalışmaları	Çok bilinen kamu sitelerine bilgi güvenliği ile ilgili sunum, materyal, derslerin konulması	Hem halk hem gençlere yönelik farkındalık amaçlı eğitim kampanyalarının düzenlenmesi,	Meslek liselerinin bilgisayarla ilgili bölümlerinde siber güvenlik konularının müfredata alınması
	Gençlerin internet alanında hatalı davranışlarının neler olduğu izlenmesi, okullarda bu davranışların dönüştürülmesi	Halka siber güvenlik konusunda kişisel önlem almaması durumunda devletin de zarar görebileceğinin açıklanması	FATİH projesi kapsamında bilgisayar kullanımına ilişkin farkındalığın oluşturulması
		Kamu-özel sektör işbirliğinin profesyonel siber güvenlik sertifikasyonları için desteklenmesi	
Farkındalık Çalışmaları	Mesleklere göre, o meslekte karşılaşılabilecek siber riskler ayırt edilmeli, meslek mensuplarına eğitimler verilmesi	Ulusal farkındalık için broşürler hazırlama, TV yayınları ile kişisel siber güvenliğe ilişkin önlemleri anlatmak	Siber güvenliğe ilişkin kursların açılması
	Kişisel olarak siber güvenliğin nasıl sağlanacağına ilişkin kamuya ait web sitelerinde bilgi ve video paylaşılması	Gençleri siber güvenlik konusunda projeler hazırlamaya yönlendirmek, özel sektör, devlet ve gençler arasında konuyla ilgili iletişimi güçlendirmek	RTÜK tarafından yayınlanan kamu spotları

Bilgi güvenliğinin oluşturulması için ilk önce durum değerlendirmesi yapılmalıdır. Hem kişisel hem organizasyonel hem de ulusal düzeyde ne tür bilgilerin var olduğunu, bunların nelerden korunması gerektiğini ve korunma için nasıl bir politika izleneceğini kararlaştırmak gerekmektedir. Süreç risk değerlendirmesi ile başlatılabilecektir. Bu aşamada misyon ve vizyon belirlenmeli, kritik altyapının durumu kontrol edilmeli ve eksiklikler tespit edilmelidir. Altyapı sorunlarının hangi bilgi güvenliği risklerine neden olabileceği araştırılmalı ve bunun için iyileştirme çalışmaları başlatılmalıdır. Risk analizi esnasında bilgi güvenliği için kullanılacak olan teknolojilerin neler olduğuna da karar verilmektedir. Bu teknolojilerden eksik olanlar tespit edilmeli, eksiklerin tamamlanması için bir planlama yapılmalıdır. Hangi güvenliği sağlama unsurlarının şart hangilerinin ise ek güvence için olacağına dair sınıflandırmaların yanı sıra bunun arge, eğitim ve ekonomik boyutlarının da değerlendirilmesi, doğru stratejinin oluşturulması için önem taşımaktadır. Ulusal alanda risk değerlendirilmesi yapılırken hangi bilgilerin en önemli olduğuna karar verilmeli, güvenlik sisteminin paydaşı olacak sektörler tanınmalı ve görev dağılımı gerçekleştirilmelidir [42] [68].

Farkındalığı arttırma konusunda kitlelerin belirlenmesi için hangi kurumların/paydaşların sorumlu olduğunu netleştirmek şarttır. Bu aşamada kamu, özel kuruluş ve kişilerin görev tanımlamaları yapılmaktadır. Çoğunlukla kamu kurumları güvenlik ile ilgili politikaları ve yasaların belirlenmesinde görev almakta, özel sektör ve eğitim kurumları ise kritik altyapının oluşturulmasında çalışmaktadırlar. Sivil toplum ise kişisel bilgi güvenliği önlemlerini almanın yanı sıra kitlesel farkındalığın geliştirilmesi hususunda rol sahibidir [42].

Kişilerin belirlenebilmesinin yanı sıra, farkındalığın tanımlamasının da yapılması gerekmektedir. Bilgi güvenliği farkındalığı, bilginin güvende tutulmasının öneminin, bunun güvenliğini riske atacak risklerin ve bu risklere karşı alınması gereken önlemlerin bilinmesidir. Ulusal bilgi güvenliği farkındalığı denildiğinde kurum ve bireylerin bilgi güvenliğini sağlamak için kendi üzerlerine düşenleri bilmesi anlamı ortaya çıkmaktadır [69].

Bölüm 6

Alan Araştırması

Çocuklar etraflarında gördüklerini kolaylıkla öğrenebilmektedirler. Ancak onların seviyelerine göre verilen eğitimleri oyunlarla desteklemek, yeteneklerine ve ilgi alanlarına göre eğitim planlaması yapmak kısa sürede sonuç verecektir [70]. Bu nedenle aslında çok basit ve maliyeti düşük olan girişimler ile çocuklara internet ve siber risklerin farkındalığına ilişkin bilgiyi vermek mümkün olacaktır.

AB ve ABD'deki uygulamalara bakıldığında çok küçük yaşlardan itibaren çocuklara konuya ilişkin eğitim verilmeye başlanmaktadır. Bu sayede çocuklar hem bilgisayar ve internet ile bilinçli şekilde ve gözlem altında tanıştırılmakta ve merakları uyandırılmakta hem de onların kendilerini nasıl koruyacağı açıklanmaktadır. Çocuğun yaşı ve ilgisi arttıkça eğitim planı da buna göre şekillenerek bilinç düzeyi arttırılmaktadır. Eğitim almış olan çocuk ve gençler evdeki ebeveynlerini de konuyla ilgili bilgilendirecekler ve güvenlikle ilgili uyaracaklardır.

6.1 Yöntem

Bir önceki bölümlerde her geçen gün internet kullanımın artması ile siber güvenlik problemlerinin nasıl ortaya çıktığı ve buna ilişkin yapılması gerekenleri belirttik. Ayrıca Siber güvenlik farkındalığını artırmak için geliştirdiğimiz eğitim içeriğinden de bahsettik. Bu bölümde ise uyguladığımız siber güvenlik farkındalık eğitiminin nasıl bir etki yarattığı

gösterilecektir. Bu bağlamda araştırmamızın sorusu, "geliştirmiş olduğumuz siber güvenirlik farkındalık eğitiminin ortaokul öğrencilerinde kişisel siber güvenliği sağlama ve siber zorbalığı farkındalıkta pozitif etkisi var mıdır?"

6.2 Araştırma Modeli

Araştırmamızın temel amacı ve sorusu siber güvenirlik için geliştirdiğimiz eğitim modülünün nasıl bir etki sağladığını ölçebilmektir bu amaçla belirlemiş olduğumuz örnekleme eğitimden önce bir yazılı anket uygulanarak onların siber güvenirlik ve duyarlılıkları ölçülecektir. Daha sonra öğrencilere belirlemiş olduğumuz eğitim uygulanacaktır. Eğitim bittikten sonra 30 dakika ara verilecek ve başta uygulamış olduğumuz ölçekler öğrencilere tekrar uygulanacaktır. Böylelikle eğitimin öğrenciler üzerinde nasıl bir etkisi olduğu gözlemlenecektir. Araştırmamızın hipotezleri ise şu şekildedir; H1: Geliştirilen eğitim modülünün ortaokul öğrencilerinin "kişisel gizliliğini koruma" üzerinde etkisi vardır. H2: Geliştirilen eğitim modülünün ortaokul öğrencilerin "internette güvenilmeyenden kaçınma" üzerinde etkisi vardır. H3: Geliştirilen eğitim modülünün ortaokul öğrencilerin "internette önlem alma" üzerinde etkisi vardır. H4: Geliştirilen eğitim modülünün ortaokul öğrencilerin "internette iz bırakma" üzerinde etkisi vardır. H5: Geliştirilen eğitim modülünün ortaokul öğrencilerin siber zorbalığa ilişkin duyarlı olmasında etkili olmuştur.

6.3 Veri Toplama Araçları

Araştırmamızda veri toplama yöntemi olarak yazılı (klasik anket) metodu uygulanmıştır. Eğitimden önce öğrencilerden üç bölümden oluşan anket formunun cevaplanması istenirken, eğitimden sonra demografik bilgileri hariç tutularak iki bölüme ilişkin cevaplar toplanmıştır. Eğitimden önce uygulanan ankete Form-1 ve eğitimden sonra uygulanacak ankete Form-2 ismi verilmiştir. Form-1, üç kısımdan oluşmaktadır ilk kısım öğrencilerin yaş, cinsiyet, öğrenim gördüğü sınıf vb. demografik bilgilerini ayrıca internet kullanım alışkanlıklarını ölçen sorulardan oluşmaktadır. İkinci kısımda ise O. Erol, Y.L. Şahin, E. Yılmaz ve H.İ. Haseski (2005) geliştirdiği kişisel siber güvenliği sağlama ölçeği (KSGSÖ) kullanılmıştır [71]. Orijinal ölçek 25 soru ve beş faktörden oluşmaktadır bunlar sırası ile kişisel gizliliği koruma, güvenilmeyenden kaçınma, önlem alma, ödeme bilgilerini koruma ve iz bırakmadır. Uyguladığımız anket ortaokul öğrencilerine uygulanacağı için ödeme

bilgilerini koruma faktörü araştırma dışı tutulmuştur. Üçüncü bölümde ise T. Tanrıkulu, H. Kınay ve O. T. Arıcak (2013) geliştirdiği siber zorbalığa ilişkin duyarlılık ölçeği (SZİDÖ) kullanılmıştır [72]. Orijinal ölçek 13 soru ve tek faktörden oluşmaktadır. Uygulanacak eğitimden sonra öğrencilere Form 2 verilmiştir, Form 2'de yalnızca KSGSÖ ve SZİDÖ ölçeği yer almıştır.

6.4 Örneklem

2016 -2017 Milli eğitim bakanlığı verilerine göre Türkiye'de ortaokul sayısı, 17 bin 879 olmakla birlikte ortaokullardaki öğrenci sayısı ise 5 milyon 554 bin 415'dir. Diğer yandan İstanbul İl Milli Eğitim Müdürlüğü, Strateji Geliştirme bölümü 2017 raporuna göre 2016-2017 döneminde toplam 1.966.712 ortaokul öğrencisi vardır.

Çalışmaya gerçek durumu ortaya çıkaracak kadar yeterli genişlikte örneklem alınmadığında Tip II hata (β) büyür, dolayısı ile güç ($1-\beta$) küçülür. Çalışma sonucunda karşılaştırılan yöntemler arasında ister "fark var ($p<0.05$)" bulunsun, ister "fark yok ($p>0.05$)" bulunsun bu durum gerçeği yansıtmalıdır. Bunun için örneklem sayısı ve güç (power) analizi bilimsel araştırmalarda önemli rol oynamaktadır. Çalışmanın örneklem yöntemi olarak basit rastgele yöntemine karar verilmiştir. İstanbul'da yer alan bir özel ve iki devlet okulu olmak üzere toplam 3 ortaokulda araştırma yürütülmüştür. Çalışmanın zorluğu, zaman ve maliyet unsurları örnek büyüklüğünü belirlemede önemli unsurlar olmuştur. Literatürde sıkça tercih edilen yöntem olarak, soru sayısının en az 5 katı kadar örnekleme ulaşılması tavsiye edilmektedir. Toplam 36 ölçek sorusu göz önünde bulundurulduğunda en az ulaşmamız gereken örneklem miktarının 180 olduğu görülmektedir. Yapılan örneklem sonucuna göre %5 hata payında 180 ortaokul öğrencisinin seçilmesi yeterli ve uygun görülmüştür, fakat olabilecek hatalar göz önünde bulundurularak 211 ortaokul öğrencisi üzerinden veri toplanmıştır.

6.5 Verilerin Değerlendirilmesi

Veriler değerlendirilirken ilk önce ölçekler için güvenirlik analizi yapılmıştır. Yapılan güvenirlik analizleri sonucu olumlu olması durumunda normallik testi uygulanıp verimizin

normal dağılımı uyup uymadığı araştırılmıştır. Normal dağılıma uygun olması durumunda parametrik testler, diğer durumda ise non-parametrik testler uygulanarak hipotezlerimiz doğrulanacaktır. Anlamlılık düzeyi α=0.05 olarak seçilmiştir. Araştırmada kullanılan veriler bilgisayar ortamına aktarılarak SPSS 25.0 yardımıyla çözümlenmiştir. İstatistiksel çözümlemelere geçilmeden Kişisel Siber Güvenliği Sağlama Ölçeği puanlarına ilişkin güvenilirlik çalışması yapılmış ve KSGSÖ için Cronbach Alfa 0,75 değeri bulunmuştur. KSGSÖ alt boyutlarının iç tutarlığı incelendiğinde Cronbach Alpha Değerleri: kişisel güvenliği koruma için 0,80; güvenilmeyenden kaçınama için 0,72; önlem alama için 0,73 ve iz bırakma boyutu için 0,69 bulunmuştur. Siber zorbalığa ilişkin duyarlılık ölçeği güvenirlik değeri 0,91 saptanmıştır. Bu neticelerden sonra veriler güvenilir kabul edilmiş ve çözümlemelere geçilmiştir.

Araştırmada öncelikle beşinci sınıf ortaöğretim öğrencilerine yönelik demografik, aile ve internet kullanım alışkanlıklarına yönelik soruların frekans dağılımı yer almaktadır. Çözümlemelere geçilmeden önce ölçek puanlarının normallik testi yapılmış ve değişkenlerin normal dağılmadığı saptanmıştır. Çözümlemelerde iki değişken karşılaştırmasında veri testi normal dağılmadığı için non-parametrik testlerden Man Whitney U testi, ikiden fazla değişken olduğu karşılaştırmalarda non-parametrik testlerden Kruskall Wallis testi kullanılmıştır. Ayrıca eğitim öncesi ve eğitim sonrası puan karşılaştırmasında Kruskal Wallis testi uygulanmıştır. Anlamlılık düzeyi α=0.05 olarak seçilmiştir.

Bölüm 7

Bulgular

Tablo 7.1'de araştırmaya katılan öğrencilerin demografik özelliklerine ilişkin frekans tablosu yer almaktadır. Araştırmaya toplam 211 5.sınıf öğrencisi katılmıştır. Araştırmaya katılan öğrencilerin %52,1'i kız ve %47,9'u erkektir. Öğrencilerin yaş aralığı incelendiğinde %54,5'i 11-12 yaş arasında ve %45,5'i 9-10 yaş arasında olduğu saptanmıştır.

Tablo 7.1: Öğrencilerin demografik bilgileri

		n	%
Cinsiyet	Kız	110	52.1
	Erkek	101	47.9
Yaş	9-11	96	45.5
	11-12	115	54.5

Araştırma iki devlet okulu ve bir özel okul olmak üzere üç okulda yürütülmüştür. Katılımcıların yüzde 68,2'si devlet ve yüzde 31,8'i Özel Okul/kolej eğitim görmektedir.

Tablo 7.2: Öğrencilerin eğitim gördükleri okul ve türü

		n	%
Okul İsmi	Mutluhan Uzunal Çolakoğlu Ortaokulu	72	34.1
	Tekden Koleji	67	31.8
	Yavuz Selim Ortaokulu	72	34.1
Eğitim Alınan Okul Türü	Devlet	144	68.2
	Özel Okul/ Kolej	67	31.8

Tablo 7.3'de araştırmaya katılan öğrencilerin anne ve baba eğitim durumlarını göstermektedir. Öğrencilerin anne ve baba eğitim düzeyi seviyesinin birbirine oldukça yakın olduğu görülmüştür. Buna göre araştırmaya katılan öğrencilerin yüzde 6,2'sinin anne eğitim ve yüzde 6,6'sının baba eğitim düzeyi okuryazardır. Öğrencilerin yüzde 42,0'nin anne ve yüzde 41,7'sinin baba eğitim seviyesi üniversiteden mezundur.

Tablo 7.3: Öğrencilerin anne ve baba eğitim durumu

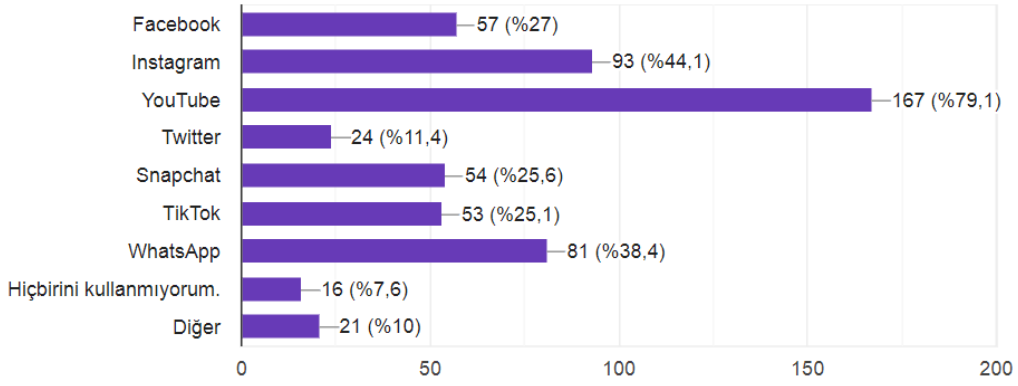
		n	%
Anne Eğitim Seviyesi	Okuryazar	13	6.2
	İlkokul	15	7.1
	Ortaokul	34	16.1
	Lise	40	19
	Üniversite	89	42
	Yüksek Lisans/Doktora	20	9.5
Baba Eğitim Seviyesi	Okuryazar	14	6.6
	İlkokul	7	3.3
	Ortaokul	28	13.3
	Lise	52	24.6
	Üniversite	88	41.7
	Yüksek Lisans/Doktora	22	10.4

Tablo 7.4 araştırmaya katılan öğrencilerin internet kullanım alışkanlıklarına ilişkin soruların frekans dağılımını göstermektedir. Buna göre araştırmaya katılan ortaokul öğrencilerinin yüzde 63,5'i 7 saatten az, yüzde 21,8'i 8-14 saat arası, yüzde 5,7'si 15-21 saat arası ve yüzde 2,8'i 22 saat ve üzeri haftalık internet kullandığı saptanmıştır. Katılımcıların yüzde 6,2si internet kullanmadığını belirtmiştir. Ortaokul öğrencilerinin yüzde 51,2'si gelecekte sosyal medya fenomeni olmayı düşünmektedir. Ayrıca öğrencilerin yüzde 14,2'si gelecekte doktor, avukat, mühendis vb. olmak yerine sosyal medya fenomeni olmayı tercih etmektedir.

TABLO 7.4: Öğrencilerin internet kullanım alışkanlıkları

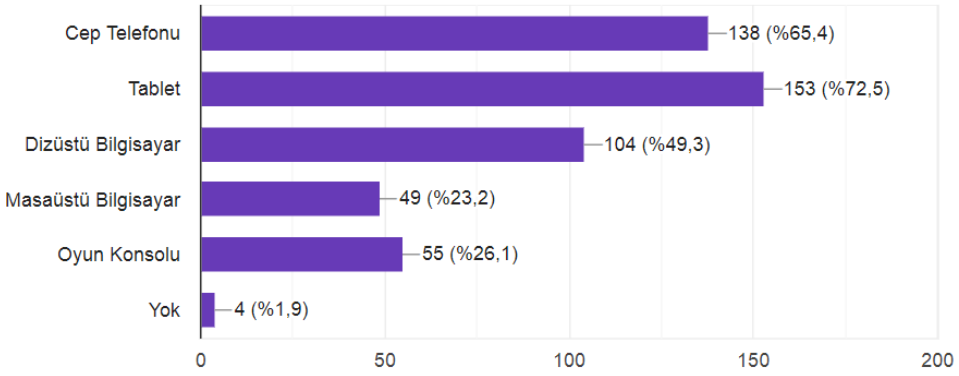
		n	%
Haftalık İnternet Kullanım Süresi	İnternet Kullanmıyorum	13	6,2
	7 saatten az	134	63,5
	8-14 Saat arası	46	21,8
	15-21 Saat arası	12	5,7
	22 Saat ve üzeri	6	2,8
Sosyal Medya Fenomeni Olma İsteği	Evet	108	51,2
	Hayır	103	48,8
Gelecekte doktor, avukat, mühendis vb. olmak yerine sosyal medya fenomeni olmayı tercih etme durumu	Kesinlikle Katılmıyorum	120	56,9
	Kararsızım	61	28,9
	Kesinlikle Katılıyorum	30	14,2

Araştırmaya katılan öğrencilerin en çok kullandığı sosyal medya sitesi YouTube (yüzde 79,1)' dur. Bu sosyal medya mecrasını Instagram takip etmektedir (yüzde 44,1). Üçüncü en çok kullanılan sosyal medya aracı ise Whatsapp (yüzde 38,4) olmuştur. Hiç sosyal medya kullanmayanların oranı ise yüzde 7,6'dır.



ŞEKIL 7.1: Ortaokul öğrencilerinin en sevdiği sosyal medya araçları.

Grafik 7.2'de araştırmaya katılan ortaokul öğrencilerinin yüzde 72,5'nin tablet, yüzde 65,4'nün cep telefonu ve yüzde 23,2'sinin masaüstü bilgisayarı olduğu saptanmıştır. Ortaokul öğrencilerinden sadece 4'nün herhangi bir kişisel cihaza sahip olmadığı saptanmıştır.



Şekil 7.2: Ortaokul öğrencilerinin kullandığı cihaz tipleri.

Araştırmaya katılan ortaokul öğrencilerinden yüzde 63,5'nin daha önce internette güvenli dolaşım ile ilgili eğitim almadığı saptanmıştır.

Tablo 7.5: Ortaokul öğrencilerinin daha önce güvenli internet eğitimi alma durumu

		n	%
İnternette Güvenli Dolaşım ile İlgili eğitim Alma Durumu	Evet, Eğitim aldım	77	36,5
	Hayır, Eğitim almadım	134	63,5

Yansız bir tahmin yapabilmek için öğrencilerin eğitimden önceki bazı özellikleri arasında fark olmaması beklenir. Bu bölümde eğitimden önce hesaplanan KSGSO ve SZİDÖ puanlarının öğrencilerin farklı demografik ve kişisel özelliklerine göre anlamlı farklılık göstermemesi beklenir.

Tablo 7.6'da araştırmaya katılan ortaokul öğrencilerinin KSGSÖ alt boyut ve SZİDÖ puanlarının cinsiyetlerine göre değişimi non parametrik testlerden Man Whitney U testi ile araştırılmıştır. Yapılan testin sonucuna göre Kişisel gizliliği koruma, Güvenilmeyenden kaçınma, Önlem alma ve İz bırakma rank ortalamaları cinsiyete göre anlamlı farklılık göstermemiştir ($p>0,05$). Dolayısıyla cinsiyet faktörü kişisel siber güvenliği üzerine etkili olmamıştır. Ortaokul öğrenicilerinin SZİDÖ rank ortalaması cinsiyete göre istatistiksel olarak farklılık göstermemiştir ($t= -1,690$; $p>0,05$). Sonuç olarak eğitimden önce ortaokul öğrencilerinin siber güvenliğe ve siber zorbalığa ilişkin bilgileri cinsiyete göre değişmemektedir.

Tablo 7.6: Eğitimden önce kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin ortaokul öğrencilerinin cinsiyetine göre değişimi

	Cinsiyet								Test Sonucu	
	Kız (n=110)				Erkek(n=101)					
	Ort.	S.S.	Med	Range	Ort.	S.S.	Med	Range	MW	P
Kişisel Gizliliği Koruma	17,21	6,00	16,00	34,00	19,84	8,31	17,00	36,00	-2,028	0,053
Güvenilmeyenden Kaçınma	15,38	4,23	16,00	16,00	14,38	4,56	16,00	16,00	-1,582	,144
Önlem Alma	18,99	4,57	20,00	20,00	18,63	5,08	19,00	20,00	-,283	,777
İz Bırakma	15,06	3,67	15,50	16,00	13,23	4,06	14,00	16,00	-2,208	,051
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	53,06	10,70	55,00	52,00	49,98	12,72	52,00	52,00	-1,690	,091

Tablo 7.7'de araştırmaya katılan ortaokul öğrencilerinin KSGSÖ alt boyut ve SZİDÖ puanlarının yaş grubuna göre değişimi non parametrik testlerden Man Whitney U testi ile araştırılmıştır. Yapılan testin sonucuna göre Kişisel gizliliği koruma, Güvenilmeyenden kaçınma, Önlem alma ve İz bırakma rank ortalamaları ortaokul öğrencilerinin yaş grubuna göre anlamlı farklılık göstermemiştir (p>0,05). Yaş grubu faktörü kişisel siber güvenliği üzerine etkili olmamıştır. Ortaokul öğrenicilerinin SZİDÖ rank ortalaması yaş grubuna göre istatistiksel olarak farklılık göstermemiştir (t= -0,313; p>0,05). Sonuç olarak eğitimden önce ortaokul öğrencilerinin siber güvenliğe ve siber zorbalığa ilişkin bilgileri yaş grubuna göre değişmemektedir.

Tablo 7.7: Eğitimden önce kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin ortaokul öğrencilerinin yaş grubuna göre değişimi

	Yaş									
	9-10 (n=96)				11-12 (n=115)				Test Sonucu	
	Ort.	S.S.	Med	Range	Ort.	S.S.	Med	Range	MW	P
Kişisel Gizliliği Koruma	18,50	7,15	16,00	32,00	18,44	7,46	17,00	36,00	-,034	,973
Güvenilmeyenden Kaçınma	14,69	4,61	16,00	16,00	15,08	4,26	16,00	16,00	-,467	,640
Önlem Alma	18,17	4,64	19,00	19,00	19,37	4,91	20,00	20,00	-2,100	,056
İz Bırakma	14,04	3,95	14,00	16,00	14,30	3,98	15,00	16,00	-,561	,575
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	51,67	12,32	54,50	52,00	51,52	11,37	53,00	50,00	-,313	,754

Tablo 7.8 'de araştırmaya katılan ortaokul öğrencilerinin KSGSÖ alt boyut ve SZİDÖ puanlarının eğitim alınan okul türüne göre değişimi non parametrik testlerden Man Whitney U testi ile araştırılmıştır. Yapılan testin sonucuna göre Kişisel gizliliği koruma, Güvenilmeyenden kaçınma, Önlem alma ve İz bırakma rank ortalamaları ortaokul öğrencilerinin eğitim alınan okul türüne göre anlamlı farklılık göstermemiştir (p>0,05). Eğitim alınan okul özel veya devlet olması faktörü kişisel siber güvenliği üzerine etkili bir etken değildir.

Ortaokul öğrenicilerinin SZİDÖ rank ortalaması eğitim alınan okul türüne göre istatistiksel olarak farklılık göstermemiştir (t= -0,200; p>0,05). Sonuç olarak eğitimden önce ortaokul öğrencilerinin siber güvenliğe ve siber zorbalığa ilişkin bilgileri eğitim alınan okul türüne göre değişmemektedir.

Tablo 7.8: Eğitimden önce kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin ortaokul öğrencilerinin eğitim durumuna göre değişimi

	Eğitim Alınan Okul Türü								Test Sonucu	
	Devlet (n=144)				Özel Okul/ Kolej (n=67)					
	Ort.	S.S.	MW	P	Ort.	S.S.	Med	Range	MW	P
Kişisel Gizliliği Koruma	18,20	6,91	16,00	36,00	19,04	8,12	16,00	34,00	-,322	,748
Güvenilmeyenden Kaçınma	14,87	4,37	16,00	16,00	14,97	4,53	16,00	16,00	-,267	,790
Önlem Alma	18,63	4,92	19,00	20,00	19,22	4,60	20,00	20,00	-,762	,446
İz Bırakma	13,94	4,03	14,00	16,00	14,72	3,79	15,00	14,00	-1,310	,190
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	51,46	11,84	53,00	52,00	51,87	11,74	54,00	52,00	-,200	,841

Tablo 7.9 'da araştırmaya katılan ortaokul öğrencilerinin KSGSÖ alt boyut ve SZİDÖ puanlarının internette güvenli dolaşım ile ilgili eğitim alma durumuna göre değişimi non parametrik testlerden Man Whitney U testi ile araştırılmıştır. Yapılan testin sonucuna göre Kişisel gizliliği koruma, Güvenilmeyenden kaçınma, Önlem alma ve İz bırakma rank ortalamaları ortaokul öğrencilerinin internette güvenli dolaşım ile ilgili eğitim alma durumuna göre anlamlı farklılık göstermemiştir (p>0,05). Ortaokul öğrenicilerinin SZİDÖ rank ortalaması internette güvenli dolaşım ile ilgili eğitim alma durumuna göre istatistiksel olarak farklılık göstermemiştir (t= -0,200; p>0,05). Sonuç olarak eğitimden önce ortaokul öğrencilerinin siber güvenliğe ve siber zorbalığa ilişkin bilgileri internette güvenli dolaşım ile ilgili eğitim alma durumuna göre değişmemektedir.

Tablo 7.9: Eğitimden önce kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin ortaokul öğrencilerinin internette güvenli dolaşım ile ilgili eğitim alma durumuna göre değişimi

	İnternette Güvenli Dolaşım ile İlgili eğitim Alma Durumu								Test Sonucu	
	Evet, Eğitim aldım (n=77)				Hayır, Eğitim almadım (n=134)					
	Ort.	S.S.	Med	Range	Ort.	S.S.	Med	Range	MW	P
Kişisel Gizliliği Koruma	18,05	7,50	16,00	34,00	18,71	7,21	17,00	36,00	-1,060	,289
Güvenilmeyenden Kaçınma	14,88	4,21	15,00	16,00	14,91	4,54	16,00	16,00	-,278	,781
Önlem Alma	19,91	4,20	21,00	15,00	18,19	5,04	19,00	20,00	-2,001	0,55
İz Bırakma	14,78	3,80	15,00	12,00	13,84	4,03	14,00	16,00	-1,545	,122
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	52,57	10,95	54,00	52,00	51,02	12,24	53,50	52,00	-722	,470

Tablo 7.10' da araştırmaya katılan ortaokul öğrencilerinin KSGSÖ alt boyut ve SZİDÖ puanlarının anne eğitim durumu değişkenine göre değişiklik gösterip göstermediği non-parametrik testlerden Kruskall Wallis ile araştırılmıştır. Yapılan testin sonucuna göre hiçbir KSGSÖ alt boyutu ve SZİDÖ rank ortalaması, öğrencilerin anne eğitim durumu grupları arasında istatistiksel olarak anlamlı farklılık görülmemiştir ($p>0,05$). Dolayısıyla eğitimden önce KSGSÖ alt boyut ve SZİDÖ puanları öğrencilerin anne eğitim durumuna göre değişmemektedir.

TABLO 7.10: Eğitimden önce kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin ortaokul öğrencilerinin anne eğitim durumuna göre değişimi

		Anne Eğitim Seviyesi					
		Ort.	S.S.	Med	Range	X^2	P
Kişisel Gizliliği Koruma	Okur Yazar	20,15	7,05	17,00	25,00		
	İlkokul	19,87	4,82	20,00	17,00		
	Ortaokul	20,47	8,91	17,50	31,00	9,039	,108
	Lise	18,62	6,53	17,50	32,00		
	Üniversite	17,18	6,83	16,00	36,00		
	Yüksek Lisans/Doktora	18,35	9,00	16,00	34,00		
Güvenilmeyenden Kaçınma	Okur Yazar	14,62	3,45	14,00	11,00		
	İlkokul	13,53	4,22	14,00	16,00	4,410	,492
	Ortaokul	14,35	5,11	16,00	16,00		
	Lise	14,45	5,03	16,00	15,00		
	Üniversite	15,36	3,97	16,00	16,00		
	Yüksek Lisans/Doktora	15,90	4,45	17,00	13,00		
Önlem Alma	Okur Yazar	18,46	4,05	21,00	13,00		
	İlkokul	17,93	6,49	21,00	20,00		
	Ortaokul	19,35	5,12	20,50	20,00	10,401	,065
	Lise	17,02	4,43	17,50	16,00		
	Üniversite	19,58	4,74	20,00	20,00		
	Yüksek Lisans/Doktora	19,00	3,71	20,00	15,00		
İz Bırakma	Okur Yazar	14,85	2,76	16,00	9,00		
	İlkokul	13,33	4,73	13,00	15,00	7,508	,186
	Ortaokul	13,68	4,48	15,00	16,00		
	Lise	12,95	3,88	13,50	16,00		
	Üniversite	14,93	3,69	15,00	14,00		
	Yüksek Lisans/Doktora	14,40	4,03	15,00	12,00		
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	Okur Yazar	51,15	12,08	50,00	38,00		
	İlkokul	49,67	12,35	49,00	40,00		
	Ortaokul	50,18	12,68	53,50	52,00	1,319	,933
	Lise	52,30	11,76	54,00	48,00		
	Üniversite	52,34	11,22	54,00	50,00		
	Yüksek Lisans/Doktora	50,95	13,17	55,50	52,00		

Tablo 7.11'de araştırmaya katılan ortaokul öğrencilerinin KSGSÖ alt boyut ve SZİDÖ puanlarının baba eğitim durumu değişkenine göre değişiklik gösterip göstermediği non-parametrik testlerden Kruskall Wallis ile araştırılmıştır. Yapılan testin sonucuna göre hiçbir KSGSÖ alt boyutu ve SZİDÖ rank ortalaması, öğrencilerin baba eğitim durumu grupları arasında istatistiksel olarak anlamlı farklılık görülmemiştir ($p>0,05$). Dolayısıyla

eğitimden önce KSGSÖ alt boyut ve SZİDÖ puanları öğrencilerin baba eğitim durumuna göre değişmemektedir.

TABLO 7.11: Eğitimden önce kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin ortaokul öğrencilerinin baba eğitim durumuna göre değişimi

		Baba Eğitim Seviyesi					
		Ort.	S.S.	Med	Range	X^2	P
Kişisel Gizliliği Koruma	Okur Yazar	21,21	7,23	19,50	24,00		
	İlkokul	16,71	5,31	18,00	14,00		
	Ortaokul	19,14	7,38	17,50	30,00	4,493	,481
	Lise	18,42	7,05	16,00	32,00		
	Üniversite	18,08	7,31	16,00	36,00		
	Yüksek Lisans/Doktora	18,09	8,56	15,00	34,00		
Güvenilmeyenden Kaçınma	Okur Yazar	14,36	4,50	14,00	15,00		
	İlkokul	13,43	5,83	15,00	16,00		
	Ortaokul	13,71	4,14	14,00	16,00	4,721	,451
	Lise	15,04	4,44	16,00	15,00		
	Üniversite	15,26	4,35	16,00	16,00		
	Yüksek Lisans/Doktora	15,45	4,55	16,00	13,00		
Önlem Alma	Okur Yazar	18,14	4,83	20,50	15,00		
	İlkokul	16,43	7,18	16,00	20,00	4,361	,499
	Ortaokul	17,64	4,78	18,00	20,00		
	Lise	19,19	4,81	20,50	16,00		
	Üniversite	19,20	4,96	19,50	20,00		
	Yüksek Lisans/Doktora	19,09	3,15	19,50	13,00		
İz Bırakma	Okur Yazar	14,64	3,54	15,00	12,00		
	İlkokul	11,14	4,56	10,00	12,00	6,951	,224
	Ortaokul	13,61	3,81	14,00	16,00		
	Lise	13,88	4,16	15,00	16,00		
	Üniversite	14,84	3,91	15,00	14,00		
	Yüksek Lisans/Doktora	13,68	3,63	13,00	12,00		
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	Okur Yazar	48,71	11,43	47,50	38,00		
	İlkokul	49,14	11,42	50,00	36,00	5,682	,338
	Ortaokul	48,61	12,21	50,50	40,00		
	Lise	52,54	12,17	55,00	50,00		
	Üniversite	51,98	12,02	53,50	52,00		
	Yüksek Lisans/Doktora	54,18	9,57	55,50	30,00		

TABLO 7.12: Eğitimden önce kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin ortaokul öğrencilerinin internet kullanım süresi durumuna göre değişimi

	İnternet Kullanım Süresi						
		Ort.	S.S.	Med	Range	X2	P
Kişisel Gizliliği Koruma	İnternet Kullanmıyorum	15,46	4,58	14,00	15,00		
	7 saatten az	18,43	7,51	16,50	36,00	3,358	,500
	8-14 Saat arası	18,91	7,12	16,50	30,00		
	15-21 Saat arası	19,42	8,03	18,50	21,00		
	22 Saat ve üzeri	20,50	7,69	19,00	20,00		
Güvenilmeyenden Kaçınma	İnternet Kullanmıyorum	15,54	4,61	16,00	12,00		
	7 saatten az	15,49	4,26	16,00	16,00		
	8-14 Saat arası	13,89	4,75	16,00	16,00	8,300	,110
	15-21 Saat arası	13,67	3,50	13,00	11,00		
	22 Saat ve üzeri	10,50	2,66	11,00	7,00		
Önlem Alma	İnternet Kullanmıyorum	16,85	6,04	17,00	19,00		
	7 saatten az	19,27	4,51	20,00	20,00	3,810	,432
	8-14 Saat arası	18,28	5,18	19,00	20,00		
	15-21 Saat arası	19,00	4,94	19,00	12,00		
	22 Saat ve üzeri	16,83	5,12	17,00	14,00		
İz Bırakma	İnternet Kullanmıyorum	14,38	3,95	16,00	12,00		
	7 saatten az	14,50	3,97	15,00	16,00	3,688	,450
	8-14 Saat arası	13,50	3,94	14,00	15,00		
	15-21 Saat arası	14,00	3,67	13,50	12,00		
	22 Saat ve üzeri	12,33	4,68	10,50	12,00		
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	İnternet Kullanmıyorum	48,23	16,11	53,00	52,00		
	7 saatten az	52,90	11,08	55,00	52,00	6,503	,165
	8-14 Saat arası	48,87	12,49	51,00	50,00		
	15-21 Saat arası	53,08	11,45	54,50	34,00		
	22 Saat ve üzeri	47,33	9,07	43,50	21,00		

Tablo 7.12'de araştırmaya katılan ortaokul öğrencilerinin KSGSÖ alt boyut ve SZİDÖ puanlarının internet kullanım süresine göre değişimi non parametrik testlerden Kruskall Wallis testi ile araştırılmıştır. Yapılan testin sonucuna göre Kişisel gizliliği koruma, Güvenilmeyenden kaçınma, Önlem alma ve İz bırakma rank ortalamaları ortaokul öğrencilerin internet kullanım süresine göre anlamlı farklılık göstermemiştir (p>0,05). Ortaokul öğrenicilerinin SZİDÖ rank ortalaması internet kullanım süresine göre istatistiksel olarak farklılık göstermemiştir (X^2= 6,503; p>0,05). Sonuç olarak eğitimden önce ortaokul öğrencilerinin siber güvenliğe ve siber zorbalığa ilişkin bilgileri internet kullanma süresine göre değişmemektedir.

TABLO 7.13: Eğitimden önce kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin ortaokul öğrencilerinin internet kullanım süresi durumuna göre değişimi

		İnternet Kullanım Süresi					
		Ort.	S.S.	Med	Range	X^2	P
Kişisel Gizliliği Koruma	İnternet Kullanmıyorum	15,46	4,58	14,00	15,00		
	7 saatten az	18,43	7,51	16,50	36,00	3,358	,500
	8-14 Saat arası	18,91	7,12	16,50	30,00		
	15-21 Saat arası	19,42	8,03	18,50	21,00		
	22 Saat ve üzeri	20,50	7,69	19,00	20,00		
Güvenilmeyenden Kaçınma	İnternet Kullanmıyorum	15,54	4,61	16,00	12,00		
	7 saatten az	15,49	4,26	16,00	16,00		
	8-14 Saat arası	13,89	4,75	16,00	16,00	8,300	,110
	15-21 Saat arası	13,67	3,50	13,00	11,00		
	22 Saat ve üzeri	10,50	2,66	11,00	7,00		
Önlem Alma	İnternet Kullanmıyorum	16,85	6,04	17,00	19,00		
	7 saatten az	19,27	4,51	20,00	20,00	3,810	,432
	8-14 Saat arası	18,28	5,18	19,00	20,00		
	15-21 Saat arası	19,00	4,94	19,00	12,00		
	22 Saat ve üzeri	16,83	5,12	17,00	14,00		
İz Bırakma	İnternet Kullanmıyorum	14,38	3,95	16,00	12,00		
	7 saatten az	14,50	3,97	15,00	16,00	3,688	,450
	8-14 Saat arası	13,50	3,94	14,00	15,00		
	15-21 Saat arası	14,00	3,67	13,50	12,00		
	22 Saat ve üzeri	12,33	4,68	10,50	12,00		
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	İnternet Kullanmıyorum	48,23	16,11	53,00	52,00		
	7 saatten az	52,90	11,08	55,00	52,00	6,503	,165
	8-14 Saat arası	48,87	12,49	51,00	50,00		
	15-21 Saat arası	53,08	11,45	54,50	34,00		
	22 Saat ve üzeri	47,33	9,07	43,50	21,00		

Bir önceki kısımda eğitimden önce her öğrencinin eşit seviyede olup olmadığı araştırılmıştır. Çıkan sonuca göre eğitim öncesi her öğrenci aynı seviyede internet bilgisine sahip demografik ve ailesel faktörlerinde bu bilgide farklılık yaratmadığı gözlemlenmiştir.

Başlangıç noktası aynı olan öğrencilere eğitim öncesi ve eğitim sonrası KSGSÖ alt boyut ve SZİDÖ puanın nasıl değiştiği non-parametrik testlerden Wilcoxon Signed test ile araştırılmıştır. Tablo detaylı incelendiğinde Kişisel gizliliği koruma ortalaması 18,47'den 17,63 düşmüştür. Bu değişimi istatistiksel olarak anlamlı bulunmuştur (z=-3,563 $p<0,001$). Bu sonuca göre ortaokul öğrencileri eğitimden sonra kişisel gizliliği korumaya yönelik bilgilerini artırdığı saptanmıştır. KSGSÖ ikinci alt boyutu Güvenilmeyenden kaçınma eğitim

öncesinde 14,90 iken eğitimden sonra 15,30 çıkmıştır fakat bu artış istatistiksel olarak anlamlı düzeyde değildir (z=-1,741, p=0,082). Ortaokul öğrencilerinin eğitimden önce önlem alma ortalaması 18,82 iken eğitim uygulandıktan sonra bu ortalama 19,19 artmış ve bu artış istatistiksel olarak anlamlı bulunmuştur (z=-1,960 p<0,05). Dolayısıyla uygulanan eğitim ortaokul öğrencilerinin internet üzerinde önlem alma durumlarını geliştirmeye yardımcı olmuştur. Son olarak KSGSÖ alt boyut ortalamalarından İz bırakma, eğitim öncesi 14,18 iken eğitimden sonra 18,82 çıkmıştır. Bu artış istatistiksel olarak anlamlı bulunmuştur (z=-2,590, p<0,05). Buna göre ortaokul öğrencileri eğitimden sonra internette iz bırakma konusunda bilgi ve seviyelerini arttırmıştır. Son olarak Siber zorbalığa ilişkin duyarlılık ölçeği puan ortalaması 51,59'dan 54,18 yükselmiştir ve bu artış istatistiksel olarak anlamlı bulunmuştur (z=-5,236p<0,001). Sonuç olarak verilen siber güvenirlik farkındalık eğitiminin ortaokul öğrencileri üzerinde kişisel siber güvenliği sağlamada ve siber zorbalığı farkındalıkta pozitif etkisinin olduğu söyleyebiliriz.

Tablo 7.14: Ortaokul öğrencilerinin eğitimd öncesi ve sonrası kişisel siber güvenliği sağlama ölçeği alt boyutları ve siber zorbalığa duyarlılık ölçeğinin değişimi

	Eğitim Alınan Okul Türü									
	Eğitim Öncesi				Eğitim Sonrası				Wilcoxon Test	
	Ort.	S.S.	Med	Range	Ort.	S.S.	Med	Range	Z	P
Kişisel Gizliliği Koruma	18,47	7,30	16,00	36,00	17,63	9,34	14,00	40,00	-3,563	<0,001
Güvenilmeyenden Kaçınma	14,90	4,41	16,00	16,00	15,30	5,14	17,00	16,00	-1,741	,082
Önlem Alma	18,82	4,81	19,00	20,00	19,19	6,09	21,00	20,00	-1,960	,049
İz Bırakma	14,18	3,96	15,00	16,00	14,82	4,84	16,00	16,00	-2,590	,010
Siber Zorbalığa İlişkin Duyarlılık Ölçeği	51,59	11,78	54,00	52,00	54,18	12,20	57,00	52,00	-5,236	<0,001

Bölüm 8

Sonuç ve Öneriler

8.1 Sonuç

Bilgi, ürün üretme, hizmet geliştirme, akademik ve bilimsel başarı sağlamanın yanı sıra günümüzde ekonomik süreklilik ve askeri güç için de şarttır. Ülkelerin bilim, teknik, askeri güç alanlarında tam bağımsızlığını korumaları için bilgi üretmeleri ve bunu korumaları şarttır.

Bilginin üretilmesi ve korunarak güvenliğinin sağlanması için teknik altyapının kurulması, sürekli kontrol edilmesi ve geliştirilmesi gerekir ve bunun da ön koşulu konuyu bilmektir. Hem halk hem kamu kurumları ve özel kuruluşlar hem de öğrenciler bilgi güvenliği konusunda bilinçlendirildiğinde, kişisel verilerden devlet sırlarına kadar bilginin korunması daha mümkün olacaktır. Teknik altyapı oluşumları geliştirilecek, riskler belirlenecek ve bilgi korunarak yeni bilgi oluşumu desteklenecektir.

Çalışmada görüldüğü üzere hem Avrupa Birliği hem de Amerika Birleşik Devletleri bilgi güvenliğini sağlama konusunda oldukça yoğun çalışmaktadırlar. AB'nin ve ABD'nin ilkokul döneminden başlayarak üniversiteye kadar eğitim programlarında siber güvenlik sistemlerine ilişkin öğretim planlamalarının olduğu göze çarpmaktadır [44]. Bununla birlikle hem ülkenin siber güvenliğinin sağlanması hem de halkın bilinç düzeyinin yükseltilmesi için çalışan pek çok devlete ya da sivil topluma bağlı oluşum mevcuttur [42] [56] [44]. Devlet teşkilatlanması ile farkındalık ve eğitim çalışmaları konusunda pek çok proje ve iş birliği kurmaktadırlar. AB ve ABD gençlerin siber güvenlik, siber uzay ve bilgi biriktirme konusunda eğitimlerine çok fazla önem vermektedirler. İlkokuldan üniversiteye kadar her

noktada bilgisayar kullanımı ve bilgi güvenliği konusunda eğitim ve çalıştayların devam ettiği görülmektedir.

Ancak Türkiye'de durum biraz farklıdır. Bilgi güvenliğine ilişkin oluşturulan politikalara bakıldığında, eğitimlerin teknik lise ve üniversitelerin ilgili kurumlarında verildiği görülecektir ki bu oldukça yetersizdir [41]. Bununla birlikte, halkın farkındalığının arttırılması konusunda da çalışmaların arttırılmasının gerekliliği ortaya çıkmıştır. Özellikle kamu spotları ile arttırılmaya çalışılan farkındalık için, teşviklerin arttırılması ve sivil toplum kuruluşlarının yardımlarının alınması şarttır [12].

Araştırma bölümü göstermiştir ki, çocuklar yoğun şekilde internet kullanmakta ancak onun zararlarına karşı korumasız kalmaktadırlar. Çok küçük yaşlarda çocuklar teknoloji ile tanışmakta ancak kısa sürede bunu kullanmayı bir bağımlılığa dönüştürmektedirler. Kendilerine yapılan zorbalığı fark etmedikleri gibi, birilerine zorbalık yaptıklarını da anlayamamaktadırlar. Yaşlarına uygun olmadığı halde sosyal medya platformlarını kullanmaktadırlar. Sosyal medyadan gelebilecek tehlikelerin farkında olmadıkları gibi parola belirleme, yabancılarla görüşme, kaynağı belli olmayan linklere tıklama konusunda da oldukça bilinçsizdirler. Tüm bunlar çocukları çeşitli suçlara maruz kalma ya da bu suçları işleme konusunda korunmasız hale getirmektedir.

Karacı ve Bilgici tarafından yapılan bir çalışmanın da sonuçları bu bulguyu desteklemektedir. Araştırmacılar, üniversite düzeyindeki gençler üzerinde yaptıkları araştırmada, gençlerin ilköğretim ve ortaöğretim döneminde çok uzun süre internet kullanmış olmalarına karşın henüz yeterli güvenlik bilgisine sahip olmadıklarını görmüşlerdir [73]. Bu çalışmada da 45 dakikalık bir bilinçlendirme eğitimi verilmiş ve eğitim öncesi katılan öğrencilere yapılan anket çalışmasında kişisel gizliliği koruma, önlem alma, iz bırakma, siber zorbalığa ilişkin yapılan ölçümlerle, eğitim sonrası yapılan ölçümler arasında farkındalığın anlamlı olarak arttığı görülmüştür. Sonuç olarak, verilen siber güvenlik farkındalık eğitiminin ortaokul öğrencilerinin üzerinde kişisel siber güvenliği sağlama ve siber zorbalığı farkındalıkta pozitif etkisi olduğu görülmüştür.

8.2 Öneriler

Araştırmada görüldüğü üzere bilgi bugün kişi, kurum ve ulusları güçlü kılan en önemli kaynaklar arasındadır. Bu nedenle hemen her gruptan kişi ve kurum, siber tehditler ile

karşılaşmaktadır. Bu tehditlerin önlenememesi söz konusu olduğunda, kişisel bilgilerin, kurumların gizli kalmasını istedikleri verilerinin ve ulusların kararları ve politikalarının, askeri güçlerinin ve araştırma geliştirme çalışmalarının dışarı sızma, yok edilme ya da değiştirilme riski ortaya çıkmaktadır.

Türkiye'ye ait bilgi güvenliği politikalarının eğitim ve farkındalık özelinde Avrupa Birliği ve Amerika Birleşik Devletleri ile karşılaştırıldığı bu çalışmada, ortaya çıkan en büyük önceliğin insanların ilgisinin konuya çekilmesi gerekliliği olduğu görülmektedir. Sokaktaki vatandaştan, kurum karar vericilerine kadar herkesin bilginin önemi konusunda bilinçlendirilmesi bu kaynağın en doğru şekilde kullanılması açısından önemlidir. Bilginin kullanılmasının insanların ekonomik, kültürel ve bilimsel alanlarda geliştirilmesinin ana maddesi olduğu anlatılmalıdır.

Bilginin güvenliğinin nasıl sağlanacağı ve bunun için önlem alınmadığı takdirde ne tür sorunların ortaya çıkabileceğinin de insanlara anlatılması önemlidir. Virüs yakalayan yazılımlar, şifreleme yöntemleri gibi teknolojinin yardımı ile alınabilecek önlemlerin yanı sıra kişinin kendi bilgilerini paylaşırken nelere dikkat etmesi gerektiği konusunda da eğitilmesi gereklidir. Avrupa ve ABD'de, farkındalık konusunda sivil toplumun üzerine fazlaca görev düştüğü görülmektedir. Ayrıca buralarda okullarda her seviyeden öğrenciye de konuyla ilgili ders verilmektedir. Ancak Türkiye'nin farkındalık geliştirme konusunda daha fazla aktivite gerçekleştirmesi gerektiği de görülmektedir. Yalnızca meslek liseleri ve bilgisayar ile ilgili teknik eğitim veren üniversitelerin dışında, kamunun da bilgilendirilmesi için broşür dağıtma, sivil toplumu güçlendirme ve eğitim çalışmalarını arttırma gerekmektedir.

Türkiye'nin hangi bilgileri saklamak, hangi önlemleri almak ve kimleri bilgi güvenliği konusunda yetiştirerek dünya genelinde söz sahibi bir ülkeye dönüşmek konusunda hedeflerini belirlemesi, stratejilerini de buna göre geliştirmesi yerinde bir adım olacaktır. Gençlerin bilgi güvenliğini sağlama konusunda teknik bilgiye de ihtiyaçları vardır. Bu sayede bu sektörde ekonomik güç de elde edilmiş olacaktır. Ayrıca güvenliği sağlama konusunda yerli teknolojilerin kullanılması, riskleri de düşürecektir. Farklı ülke menşeli yazılımların tercih edilmesi, her zaman yazılımcı ülkelerin müdahale riskini de beraberinde getirmektedir.

Türkiye siber stratejisi belirlenirken; bilgi güvenliğinin idamesi ve siber uzayın faydalarının azaltılmaması göz önünde bulundurulmalıdır. Bunun sağlanması için ise genç

beyinlerin gücünden faydalanmak şarttır. Çocukların küçük yaştan itibaren kod yazma, güvenliği sağlama, bunun önemi konusunda bilgilendirilmeye başlanması, teknolojinin en yüksek verimle kullanılması açısından önem taşımaktadır.

Teknolojide gerçekleşen bir yeniliğin baş döndürücü hızına ayak uydurmak ancak ve ancak üniversitelerin konu ile ilgili donanımlı hale getirilmesi ile mümkün olacaktır ve bilgi güvenliği her alanda şarttır. Güvenliğe ilişkin önlemler yalnızca mesleği bilgisayar ile uğraşmak olanlar tarafından değil, her sektörden çalışan tarafından bilinmelidir. Bu nedenle, okullarda güvenlik risklerini ölçme ve bunları engelleme konusunda çalışmalar arttırılmalı, uygulamalı dersler oluşturularak gençlerin dikkatini çekmek gerekmektedir. Öncelikli olarak ilk ve orta dereceli okullarda siber güvenlik eğitimleri ders müfredatlarına eklenmelidir. Bireysel siber güvenlik riskleri bu eğitimlerle asgari düzeye indirilecek ve ulusal siber güvenlik riski de doğru orantılı olarak düşüş gösterecektir.

Bu çalışmada Türkiye, AB ve ABD'deki siber güvenliğe ilişkin bilinçlendirme ve eğitim stratejilerinin kıyaslaması yapılmış, Türkiye'nin diğer ülkelere göre konuyu yeterince ele almadığı görülmüştür. Yalnızca liselerin bilgisayar ile ilgili kısımlarında çocuklara siber güvenlik eğitimi vermek, diğerlerini internet ortamında yalnız bırakmak anlamına gelecektir ve ilerleyen yılların karar vericisi, çalışanı ya da ebeveyni olacak olan bu çocuklar içinde bulundukları yapı için de bilgi güvenliğini bilmeye ihtiyaç duymaktadırlar. Ancak incelenen mevzuat ve stratejik hedeflerden anlaşıldığı kadarıyla ülkemizde, çocukların ilgi alanlarına göre seçmiş oldukları bölümlerde konu anlatılmaktadır. Fakat acilen görülmelidir ki çocuklar ya da gençler bugün internet ve bilgisayar sistemleri ile ilgi alanları olduğu için değil, bir gündelik yaşam biçimi haline geldiği, iletişim kurdukları ve hizmet/mal alım satımı gerçekleştirebildikleri için temas halindedirler. O halde acilen eğitime yönelik stratejilerin kapsayıcı bir biçime dönüştürülmesi gerekmektedir.

Ek A

Ekler

İSTANBUL ŞEHİR ÜNİVERSİTESİ	**ANKET NO:** Bu çalışma, İSTANBUL ŞEHİR ÜNİVERSİTESİ, FEN BİLİMLERİ ENSTİTÜSÜ, BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ BÖLÜMÜ, "DÜNYADAKİ SİBER GÜVENLİK EĞİLİMLERİ DOĞRULTUSUNDA TÜRKİYE'NİN 2023 SİBER GÜVENLİK STRATEJİSİNİN İYİLEŞTİRİLMESİ İÇİN ÖNERİLER" isimli Yüksek Lisans tezi kapsamında gerçekleştirilmektedir. Sorulara yanıt verirken "( )" içerisine X ile işaretleyerek yanıtınızı verebilirsiniz Örnek: (X) Vereceğiniz yanıtların samimiyeti araştırmanın doğru sonuçlara ulaşması ve geçerliliği açısından büyük önem arz etmektedir. Katkınız ve katılımınız için teşekkür ederim. HÜSNÜ TAVLAŞ İstanbul Şehir Üniversitesi Fen Bilimler Enstitüsü	
A. DEMOGRAFİK BİLGİ FORMU ve İNTERNET ALIŞKANLIKLARI		
S1.Cinsiyet?	( ) Kız ( ) Erkek	
S2. Yaşınız?	Yaş…….. (Yazınız)	
S3. Kaçıncı sınıfta eğitim alıyorsunuz	( ) 6. Sınıf ( ) 7. Sınıf ( ) 8. Sınıf	
S4. Hangi Okulda eğitim alıyorsunuz?	( ) Devlet ( ) Özel Okul / Kolej	
S5. Anneniz eğitim seviyesi nedir?	( ) Okuryazar ( ) İlkokul ( ) Ortaokul	( ) Lise ( ) Üniversite ( ) Yüksek Lisans/Doktora
S6. Babanızın eğitim seviyesi nedir?	( ) Okuryazar ( ) İlkokul ( ) Ortaokul	( ) Lise ( ) Üniversite ( ) Yüksek Lisans/Doktora
S7. Daha önce internette güvenli dolaşım ile ilgili eğitim aldınız mı ?	( ) Evet, eğitim aldım ( ) Hayır Eğitim almadım	
S8. Haftada kaç saat internet kullanıyorsunuz?	( ) internet kullanmıyorum ( ) 7 saatten az ( ) 8-14 Saat arası	( ) 14 -21 saat arası ( ) 22 saat ve daha üzeri
S9. En sevdiğiniz sosyal medya hangisidir?	( ) Facebook ( ) Instagram ( ) YouTube ( ) Twitter	( ) Snapchat ( ) Hiçbirini beğenmiyorum ( ) Whatsapp ( ) Diğer…… yazınız…….
S10. Gelecekte sosyal medya fenomeni olmayı çok isterim?	( ) Evet ( ) Hayır	
S11. Gelecekte doktor, avukat, mühendis vb. olmak yerine sosyal medya fenomeni olmayı tercih ederim.		( ) Kesinlikle katılıyorum ( ) Kararsızım ( ) Kesinlikle Katılmıyorum
S11. En sevdiğiniz sosyal medya fenomeni kimdir?	Yazınız……	

B. KİŞİSEL SİBER GÜVENLİĞİ SAĞLAMA ÖLÇEĞİ					
Aşağıda yer alan kişisel siber güvenliği sağlama ölçeği soruları için size en uygun gelen cevapları lütfen belirtiniz. İlgili soru karşısına cevabınızı lütfen (X) olarak belirtin 5 Kesinlikle Katılıyorum, 4 katılıyorum 3; Kararsızım 2; Katılmıyorum, 1 Kesinlikle Katılmıyorum.	KESİNLİKE KATILMIYORUM	KATILMIYORUM	KARARSIZIM	KATILIYORUM	KESİNLİKLE KATILIYORUM
	1	**2**	**3**	**4**	**5**
KİŞİSEL GİZLİLİĞİ KORUMA					
1. Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım.					
2. Tanımadığım kişilerden gelen e-posta eklerini açarım					
3. Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım.					
4. İnternet ortamında gerektiğinde kişisel bilgilerimi (TC No,Doğum tarihi, GSM No vb.)paylaşırım.					
5. Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm.					
6. Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım.					
7. Unutmamak için akılda kalan kolay bir şifre belirlerim.					
8. İnternet üzerinden yer bildirimi yaparım					
9. E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım.					
10. İnternet şifrelerimin tümünün aynı olmasına dikkat ederim.					
GÜVENİLMEYENDEN KAÇINMA					
11. Güvenmediğim sitelere üye olmam					
12. İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.					
13. Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem.					
14. Güvenmediğim sitelerden dosya indirmem					
ÖNLEM ALMA					
15. Kullandığım yazılımları güncellerim.					
16. Bilgisayarımda anti virüs yazılımı bulundururum.					
17. Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim.					
18. Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım.					
19. Web tarayıcımın güvenlik ayarlarını düzenlerim.					
İZ BIRAKMA					
20. İnternette kullandığım (e-posta, sosyal ağ vb.) şifreleri değiştiririm.					
21. Web geçmişimi temizlerim.					
22. Sosyal ağ- e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım.					
23. Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim.					

C. SİBER ZORBALIĞA İLİŞKİN DUYARLILIK ÖLÇEĞİ					
Aşağıda yer alan kişisel siber zorbalığa ilişkin duyarlılık ölçeği soruları için size en uygun gelen cevapları lütfen belirtiniz. İlgili soru karşısına cevabınızı lütfen (X) olarak belirtin 5 Kesinlikle Katılıyorum, 4 katılıyorum 3; Kararsızım 2; Katılmıyorum, 1 Kesinlikle Katılmıyorum.	KESİNLİKE KATILMIYORUM	KATILMIYORUM	KARARSIZIM	KATILIYORUM	KESİNLİKLE KATILIYORUM
	1	**2**	**3**	**4**	**5**
1. İnternete girdiğimde bilgilerimin başkaları tarafından çalınabileceğini göz önünde tutarım.					
2. Sosyal paylaşım sitelerinde (Facebook, Twitter vb.) özel bilgilerimin başkaları tarafından kötü amaçlı olarak kullanılabileceğini göz önünde bulundururum.					
3. Gerçek yaşamda sorun yaşadığım insanlarla sanal ortamlarda da karşılaşmamaya çalışırım.					
4. Sanal ortamlarda başkalarının bana zarar vermemesi için bazı tedbirler alma ihtiyacı hissettiğim olur.					
5. Sanal ortamlardayken bir bilgisayar korsanının benim için de tehlike oluşturabileceğini göz önünde bulundururum.					
6. Bana zarar vermek isteyen birisinin bunu internet, cep telefonu vb. aracılığıyla da yapabileceğini düşünürüm.					
7. İnternetteki e-posta, forum siteleri vb. üyelik şifrelerimi kimseyle paylaşmam.					
8. Sanal ortamlarda küfür veya hakarette bulunan kişilerle iletişimimi keserim					
9. Görülmesini istemediğim bir resim ya da görüntümün benden habersiz olarak yayılabileceği tehlikesini düşündüğüm olur.					
10. Sanal ortamlardaki iletişimde hakkımda gerçek olmayan söylentilerin de yayılabileceğini düşünürüm.					
11. İnternete girdiğimde internetin aynı zamanda başkalarına zarar verme amacıyla kullanılabileceğini aklımda tutarım.					
12. Benimle ilgili doğru olmayan bir bilginin internette yayılması durumda ne yapacağımı düşündüğüm olur.					
13. E-posta ya da cep telefonundan kısa mesaj (SMS) yoluyla tehdit alabileceğim kişilerle sanal ortamlarda iletişimde bulunmam.					

ANKET NO:		

AŞAĞIDA YER ALAN SORULAR, ***EĞİTİM BAŞLAMADAN ÖNCE DOLDURDUĞUNUZ FORM İLE AYNIDIR***. EĞİTİMDEN SONRA SORULAR HAKKINDA GÖRÜŞÜNÜZ ***DEĞİŞEBİLİR VEYA AYNI KALABİLİR***. LÜTFEN SORULARI DİKKATLİCE TEKRAR OKUYUN VE ***ALDIĞINIZ EĞİTİMİ GÖZ ÖNÜNDE BULUNDURARAK*** TEKRAR CEVAPLAYINIZ. SORULARIN DOĞRU VEYA YANLIŞ CEVABI YOKTUR.

C. SİBER ZORBALIĞA İLİŞKİN DUYARLILIK ÖLÇEĞİ

Aşağıda yer alan kişisel siber zorbalığa ilişkin duyarlılık ölçeği soruları için size en uygun gelen cevapları lütfen belirtiniz. İlgili soru karşısına cevabınızı lütfen (X) olarak belirtin 5 Kesinlikle Katılıyorum, 4 katılıyorum 3; Kararsızım 2; Katılmıyorum, 1 Kesinlikle Katılmıyorum.	KESİNLİKE KATILMIYORUM	KATILMIYORUM	KARARSIZIM	KATILIYORUM	KESİNLİKLE KATILIYORUM
	1	**2**	**3**	**4**	**5**
14. İnternete girdiğimde bilgilerimin başkaları tarafından çalınabileceğini göz önünde tutarım.					
15. Sosyal paylaşım sitelerinde (Facebook, Twitter vb.) özel bilgilerimin başkaları tarafından kötü amaçlı olarak kullanılabileceğini göz önünde bulundururum.					
16. Gerçek yaşamda sorun yaşadığım insanlarla sanal ortamlarda da karşılaşmamaya çalışırım.					
17. Sanal ortamlarda başkalarının bana zarar vermemesi için bazı tedbirler alma ihtiyacı hissettiğim olur.					
18. Sanal ortamlardayken bir bilgisayar korsanının benim için de tehlike oluşturabileceğini göz önünde bulundururum.					
19. Bana zarar vermek isteyen birisinin bunu internet, cep telefonu vb. aracılığıyla da yapabileceğini düşünürüm.					
20. İnternetteki e-posta, forum siteleri vb. üyelik parolalarımı kimseyle paylaşmam.					
21. Sanal ortamlarda küfür veya hakarette bulunan kişilerle iletişimimi keserim					
22. Görülmesini istemediğim bir resim ya da görüntümün benden habersiz olarak yayılabileceği tehlikesini düşündüğüm olur.					
23. Sanal ortamlardaki iletişimde hakkımda gerçek olmayan söylentilerin de yayılabileceğini düşünürüm.					
24. İnternete girdiğimde internetin aynı zamanda başkalarına zarar verme amacıyla kullanılabileceğini aklımda tutarım.					
25. Benimle ilgili doğru olmayan bir bilginin internette yayılması durumda ne yapacağımı düşündüğüm olur.					
26. E-posta ya da cep telefonundan kısa mesaj (SMS) yoluyla tehdit alabileceğim kişilerle sanal ortamlarda iletişimde bulunmam.					

B. KİŞİSEL SİBER GÜVENLİĞİ SAĞLAMA ÖLÇEĞİ					
Aşağıda yer alan kişisel siber güvenliği sağlama ölçeği soruları için size en uygun gelen cevapları lütfen belirtiniz. İlgili soru karşısına cevabınızı lütfen (X) olarak belirtin 5 Kesinlikle Katılıyorum, 4 katılıyorum 3; Kararsızım 2; Katılmıyorum, 1 Kesinlikle Katılmıyorum.	KESİNLİKE KATILMIYORUM	KATILMIYORUM	KARARSIZIM	KATILIYORUM	KESİNLİKLE KATILIYORUM
	1	**2**	**3**	**4**	**5**
KİŞİSEL GİZLİLİĞİ KORUMA					
24. Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım.					
25. Tanımadığım kişilerden gelen e-posta eklerini açarım.					
26. Banka, online alışveriş sitesi gibi sitelerden gelen e-postalara (kart numarası, parola vb. istekler) itibar ederim ve anıtlarım.					
27. İnternet ortamında gerektiğinde kişisel bilgilerimi (T.C No, doğum tarihi, GSM No vb.) paylaşırım.					
28. Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm.					
29. Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım.					
30. Unutmamak için akılda kolay kalan bir parola belirlerim.					
31. İnternet üzerinden yer bildirimi yaparım					
32. E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, parola vb. istekler) cevaplarım.					
33. İnternet parolalarımın tümünün aynı olmasına dikkat ederim.					
GÜVENİLMEYENDEN KAÇINMA					
34. Güvenmediğim sitelere üye olmam.					
35. İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.					
36. Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem.					
37. Güvenmediğim sitelerden dosya indirmem					
ÖNLEM ALMA					
38. Kullandığım yazılımları güncellerim.					
39. Bilgisayarımda anti virüs yazılımı bulundururum.					
40. Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim.					
41. Parolalarımı belirlerken basit dizilimler kullanmaktan kaçınırım.					
42. Web tarayıcımın güvenlik ayarlarını düzenlerim.					
İZ BIRAKMA					
43. İnternette kullandığım (eposta, sosyal ağ vb.) parolaları değiştiririm.					
44. Web geçmişimi temizlerim.					
45. Sosyal ağ- e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım.					
46. Şahsi bilgisayarım dışında kullandığım dijital cihazlarda bilgilerimin kalmamasına dikkat ederim.					

ARAŞTIRMA ETİK KURUL KARARLARI

Toplantı Tarihi : 04.3.2019
Toplantı Sayısı : 15/2019
Toplantı Saati : 14:00
Toplantıya Katılanlar : Doç. Dr. Eda YÜCESOY (Başkan)
Prof. Dr. Nihat BULUT
Prof. Dr. Cem BEHAR
Doç. Dr. Elif ÇELEBİ
Doç. Dr. Hızır Murat KÖSE
Doç. Dr. Sinem ELKATİP HATİPOĞLU
Dr. Öğr. Üyesi Betül NİZAM
Dr. Öğr. Üyesi Eyyüp Said KAYA

Karar No : 1- İstanbul Şehir Üniversitesi Araştırma Etik Kurulu, proje yürütücüsü Hüsnü Tavlaş tarafından sunulan, " DÜNYADAKİ SİBER GÜVENLİK EĞİLİMLERİ DOĞRULTUSUNDA TÜRKİYE'NİN 2023 SİBER GÜVENLİK STRATEJİSİNİN İYİLEŞTİRİLMESİ İÇİN ÖNERİLER" isimli proje taslağını değerlendirilerek, projenin uygunluğuna karar verilmiştir.

Aşağıda isimleri ve imzaları bulunan İstanbul Şehir Üniversitesi Araştırma Etik Kurulu üyeleri, araştırmacı tarafından kurula sunulan yukarıdaki bilgiler ışığında, ekte belirtilen araştırmanın yürütülmesinde etik açıdan bir sakınca görmemektedir.

Doç. Dr. Eda YÜCESOY
Başkan

Prof. Dr. Nihat BULUT
Üye

Prof. Dr. Cem BEHAR
Üye

KATILMADI
Doç. Dr. Elif ÇELEBİ
Üye

Doç. Dr. Hızır Murat KÖSE
Üye

Dr. Betül NİZAM
Üye

Doç. Dr. Sinem ELKATİP HATİPOĞLU
Üye

Dr. Eyyüp Said KAYA
Üye

Kaynakça

[1] TÜİK. Hanehalkı bilişim teknolojileri kullanım araştırması. Technical report, 2017. URL www.tuik.gov.tr.

[2] TÜİK. Son üç ay içinde internet kullanan bireylerin interneti kişisel kullanma amaçları. Technical report, Mayıs 2017. URL http://tuik.gov.tr/VeriBilgi.do?alt_id=1028.

[3] We are social, 2018. URL https://wearesocial.com/blog/2018/01/global-digital-report-2018. Erişim Tarihi: 2018-05-05.

[4] Ş. Sağiroğlu and İ. Ç. U. Yavanoğlu. Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, 15:15–27, 2012.

[5] T. Doğan. Veri İhlali. *Tübitak Bilim ve Teknik Dergisi*, 51:30–35, 2018.

[6] Cisco. Cisco 2013 annual security report, 2018. URL https://www.cisco.com/c/dam/global/da_dk/assets/pdfs/quick_sec_overview_patrick_fedele.pdf. Erişim Tarihi: 2018-05-06.

[7] O. Çarikçi. Türkiye-de e-devlet uygulamalari üzerine bir araştırma. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, pages 95–122, 2010.

[8] E. S. A. Efendioğlu. e-devlet uygulamalarinda bilgi ve paylaşim güvenliği. *Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi*, 16:219–236, 2007.

[9] R. Gündüz and M. Zekeriya. Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 2:327–335, 2018.

[10] Cisco. The internet of things. Technical report, 6 Mayıs 2018. URL https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf.

[11] McAfee Labs. www.mcafee.com, 2018. URL `https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf`. Erişim Tarihi: 2018-05-05.

[12] BTK. 2016 - 2019 ulusal siber güvenlik stratejisi, 2016. URL `http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf`. Erişim Tarihi: 2019-05-05.

[13] Symantec. www.symantec.com, 2018. URL `https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf`. Erişim Tarihi: 2019-05-05.

[14] Türkiye Cumhuriyeti Kalkınma Bakanlığı. Bilgi toplumu stratejisi proje ve katılımcılık portalı, 2018. URL `http://www.bilgitoplumustratejisi.org/tr/doc/8a9481984680deca014bea4232490005`. Erişim Tarihi: 2019-05-05.

[15] Türk Dİl Kurumu. Eğitim, 2019. URL `http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5aed9dacec4822.90182518`. Erişim Tarihi: 2019-05-05.

[16] U. Güney and O. Güngör. Uluslararasi ilişkilerde güvenliğin dönüşümü çerçevesinde bilgi güvenliği ve siber savaş. *Karadeniz Araştırmaları Merkezi*, pages 131–146, 2017.

[17] Ş. Ş. G. Canberk. Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9:165–174, 2006.

[18] E. Çek. Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi, 2017.

[19] M. Çetinkaya. Bilgi güvenliği yönetim sistemi altyapısının değerlendirilmesi için bir test aracı geliştirilmesi, 2008.

[20] B. Türk, N. Topaloğlu, and M. H. Calp. Bilgi güvenliği kapsamında yeni bir veri şifreleme. *Bilişim Teknolojileri Dergisi*, 9:291–301, 2016.

[21] A. Babaoğlu. Kriptolojinin geçmişi bir şifreleme algoritması kullanmadan önce son kullanım tarihine bakın! *Bilim ve Teknik*, 42:24–27, 2009.

[22] O. Kara. II. dünya savaşı'ndan günümüze kriptoloji: Enigma'dan AES'e şifreleme. *Bilim Teknik*, 42:28–33, 2009.

[23] T. Henkoğlu. Kişisel verileriniz ne kadar güvende? Bilgi güvenliği kapsamında bir değerlendirme. *Türk Arşivciler Derneği Arşiv Dünyası Dergisi*, pages 46–56, 2017.

[24] R. G. Lawrence. Multiple computer networks and intercomputer communications, 1967. URL https://people.mpi-sws.org/~gummadi/teaching/sp07/sys_seminar/arpanet.pdf. Erişim Tarihi: 2019-05-05.

[25] P. Kenekayoro. The data encryption standard thirty four years later: An overview. *African Journal of Mathematics and Computer Science Research*, 3:267–269, 2010.

[26] D. Selent. Advanced encryption standard. *Rivier Academic Journal*, 6:1–14, 2006.

[27] Ş. Sağiroğlu and Y. Vural. Kurumsal bilgi güvenliği ve standartlari üzerine bir inceleme. *Gazi Üniv. Müh. Mim. Fak. Der.*, 23:507–522, 2008.

[28] M. Label. Pwc Türkiye- küresel bilgi güvenliği araştırması, 2017. URL https://www.pwc.com.tr/tr/hizmetlerimiz/risk-surec-teknoloji-hizmetleri/bilgi-guvenligi-ve-siber-guvenlik/bilgi-guvenligi-ve-siber-guvenlik-yayinlari/kuresel-bilgi-guvenligi-arastirmasi-2017/eglence-medya-ve-iletisim-sektoru.html. Erişim Tarihi: 2019-05-05.

[29] M. Şenol. Siber güçle caydırıcılık ama nası? *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2:10–17, 2016.

[30] Chip. Chip online Atatürk Havalimanı'nda conficker paniği, 2009. URL https://www.chip.com.tr/haber/ataturk-havalimani-nda-conficker-panigi_10740.html. Erişim Tarihi: 2019-05-05.

[31] NTV. Ntv haber- Ünlü virüs Atatürk Havalimanı'nda, 2009. URL https://www.ntv.com.tr/turkiye/unlu-virus-ataturk-havalimaninda,ROZRHAfklU6Zgr0pyYFlNQ. Erişim Tarihi: 2019-05-05.

[32] www.ripe.net, 2019. URL https://www.ripe.net/ripe/mail/archives/dns-wg/2015-December/003184.html. Erişim Tarihi: 2019-05-05.

[33] B. Özdal and A. B. Darıcalı. Enformasyon savaşı bağlamında Rusya Federasyonu-Türkiye ilişkilerinin analizi. *İGÜ Sos. Bil. Dergisi*, 4:19–40, 2017.

[34] BBC. Siber saldırıların arkasında Rusya olabilir, 2015. URL https://www.bbc.com/turkce/haberler/2015/12/151223_siber_saldiri. Erişim Tarihi: 2019-05-05.

[35] HAVELSAN. Havelsan aylık siber güvenlik bülteni. Technical report, 2016. URL https://www.havelsan.com.tr.

[36] Nic. Nic.tr, 2019. URL https://www.nic.tr/2015-12-DDoS-Saldirisi-Kamuoyu-Duyurusu-20151221.pdf. Erişim Tarihi: 2019-05-05.

[37] G. Kolcu. Onlar saldırdı biz fişi çektik, December 2015.

[38] Hurriyet. Hürriyet Daily News, 2019. URL http://www.hurriyetdailynews.com/health-ministry-confirms-cyberattack-attempt-on-turkish-state-hospitals-99352. Erişim Tarihi: 2019-05-05.

[39] Sağlık Bakanlığı, 2016. URL http://www.saglik.gov.tr/TR,3501/saglik-bakanligi-hastanelerine-yonelik-siber-saldiri-girisimine-iliskin-basin-aciklamasi-18052016.html. Erişim Tarihi: 2019-05-05.

[40] D. Deloitte. Global siber güvenlik yönetici bilgilendirme raporu. Technical report, 2014. URL https://www2.deloitte.com/tr/tr/pages/risk/articles/Global-Cyber-Briefing.html.

[41] BBC. BBC News, 2019. URL http://news.bbc.co.uk/2/hi/europe/6665145.stm. Erişim Tarihi: 2019-05-05.

[42] A. Aytekin. Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi, 2015.

[43] H. Çakır. Kuzey Atlantik Antlaşma Örgütü'nün (NATO) siber güvenlik stratejisinin incelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, pages 632–656, 2017.

[44] M. Kara. Siber saldırılar- siber savaşlar ve etkileri. Master's thesis, İstanbul Bilgi Üniversitesi, İstanbul, Turkey, 2013.

[45] En Son Haber. Siber saldırının ABD'ye maliyeti: 7 milyar dolar, 2016. URL http://www.ensonhaber.com/siber-saldirinin-abdye-maliyeti-7-milyar-dolar-2016-10-22.html. Erişim Tarihi: 2019-05-05.

[46] STM. 2016 Ekim-Aralık dönemi siber tehdit durum raporu. Technical report, 2016. URL https://www.stm.com.tr.

[47] Y. Xiao, G. Sun, and W. J. T. Mahjabin. A survey of distributed denial-of-service attack, prevention and mitigation tecniques. *International Journal of Distributed Sensor Networks*, 13:1–32, 2017.

[48] R. Yönak. 2016'da gerçekleştirilen siber saldırılar, 2017. URL https://www.bbc.com/turkce/haberler-38489376. Erişim Tarihi: 2019-05-05.

[49] A. B. Darıcılı. Amerika Birleşik Devletleri'nin siber kapasitesinde rol oynayan kurumsal yapılanmaların analizi. Uluslararası IX. Uludağ Uluslararası İlişkiler Kongresi: Dünya Politikasında Kriz ve Değişim, 2017.

[50] Homeland Security. About dhs, 2018. URL https://www.dhs.gov/about-dhs. Erişim Tarihi: 2019-05-05.

[51] G. Miller and B. Gellman. The washington post, 2013. URL https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html?noredirect=on&utm_term=.69fcbd22c8f4. Erişim Tarihi: 2019-05-05.

[52] A. Glass. The National Security Agency is established, Nov. 4, 1952, 2010. URL https://www.politico.com/story/2010/11/the-national-security-agency-is-established-nov-4-1952-044671. Erişim Tarihi: 2019-05-05.

[53] E. A. Alagöz. Amerika'nın yeni güvenlik stratejisi, 2015. URL http://www.bilgesam.org/incele/2032/-amerika-nin-yeni-guvenlik-stratejisi/#.WwGucEiFN1s. Erişim Tarihi: 2019-05-05.

[54] NICCS. Cybersecurity, national cybersecurity training, 2018. URL https://niccs.us-cert.gov/cybersecurity. Erişim Tarihi: 2019-05-05.

[55] National Security Agency Central Security Service. National centers of academic excellence in cyber defense, 2016. URL https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/. Erişim Tarihi: 2019-05-05.

[56] European Comission. Digital agenda for europe: key initiatives, 2010. URL http://europa.eu/rapid/press-release_MEMO-10-200_en.htm. Erişim Tarihi: 2019-05-05.

[57] S. Karabel. Avrupa birliği'nin 2016 güvenlik strateji belgesi. *Bilgesam Analiz*, pages 1–9, 2016.

[58] ENISA. www.enisa.europa.eu, 2019. URL https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month. Erişim Tarihi: 2019-05-05.

[59] G. Gürkaynak. Amerika Birleşik Devletleri ve Avrupa Birliği düzenlemeleri ile karşılaştırmalı olarak, 2019. URL http://inet-tr.org.tr/inetconf20/bildiri/39.pdf. Erişim Tarihi: 2019-05-05.

[60] M. Turhan. Siber güvenliğin sağlanması, dünya uygulamaları ve ülkemiz için çözüm önerileri, 2010. URL http://afyonluoglu.org/PublicWebFiles/Reports-TR/Uzmanlik_Tez/BTK/siber/2010%20Ocak%20Siber%20G%C3%BCvenli%C4%9Fin%20Sa%C4%9Flanmas%C4%B1.PDF. Erişim Tarihi: 2019-06-10.

[61] Türk Dil Kurumu. http://www.tdk.gov.tr, 2018. URL http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5aed9dacec4822.90182518. Erişim Tarihi: 2019-05-05.

[62] M. Çelikpala, S. Bıçakçı, and F. D. Ergün. Türkiye'de siber güvenlik, 2019. URL http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf.

[63] Resmi Gazete. Resmi Gazete, 2014. URL http://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm. Erişim Tarihi: 2019-05-05.

[64] BTK. Bilgi Teknolojileri ve İletişim Kurumu, 2019. URL https://www.btk.gov.tr/siber-guvenlik-kurulu. Erişim Tarihi: 2019-05-05.

[65] Resmi Gazete. Resmi Gazete, 2018. URL http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm. Erişim Tarihi: 2019-05-05.

[66] MEB. Fatih projesi, 2018. URL http://fatihprojesi.meb.gov.tr/. Erişim Tarihi: 2019-05-05.

[67] Radyo Televizyon Üst Kurulu. Kamu spotları, 2018. URL https://www.rtuk.gov.tr/kamu-spotlari-5029. Erişim Tarihi: 2019-05-05.

[68] H. Çakır and H. Yaşar. Kurumsal siber güvenliğe yönelik tehditler ve önlemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, pages 488–507, 2015.

[69] S. E. Erol. Siber güvenlik farkındalığı için yetenek tabanlı dinamik model. Master's thesis, Gazi Üniversitesi, Ankara, Turkey, 2016.

[70] S. Sezgin. Öğrenme ve öğretimin oyunlaştırılması: Çalışma ve eğitim için oyun tabanlı yöntem ve stratejiler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 2: 187–197, 2016.

[71] Y. L. Şahin, E. Yılmaz, and H. İ. H. O. Erol. Kişisel siber güvenliği sağlama ölçeği geliştirme çalışması, 2015. URL `https://www.researchgate.net/publication/281753925_Personal_Cyber_Security_Provision_Scale_development_study_Kisisel_Siber_Guvenligi_Saglama_Olcegi_gelistirme_calismasi`. Erişim Tarihi: 2019-05-05.

[72] O. T. Arıcak, T. Tanrıkulu, and H. Kınay. Siber zorbalığa ilişkin duyarlılık ölçeği: Geçerlik ve güvenirlik çalışması. *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, 3: 38–47, 2013.

[73] G. Bilgici, A. Karacı, and H. İ. Akyüz. Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 25:2079–2094, 2017.