İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

SİBER GÜVENLİK POLİTİKALARINDA EĞİTİM VE TÜRKİYE'NİN SİBER GÜVENLİK EĞİTİMİ POLİTİKASI

Yüksek Lisans Tezi

Burak Eskici

Haziran 2024

İSTANBUL MEDENİYET ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

SİBER GÜVENLİK POLİTİKALARINDA EĞİTİM VE TÜRKİYE'NİN SİBER GÜVENLİK EĞİTİMİ POLİTİKASI

Yüksek Lisans Tezi

Burak Eskici

Danışman

Prof. Dr. İsmail Ermağan

Eşdanışman

Doç. Dr. Muhammed Ali Aydın

Haziran 2024

TEZ JÜRİSİ ONAYI

Burak Eskici tarafından hazırlanan "Siber Güvenlik Politikalarında Eğitim Ve Türkiye'nin Siber Güvenlik Eğitimi Politikası" başlıklı bu Yüksek Lisans Tezi, Uluslararası İlişkiler Anabilim Dalı'nda hazırlanmış ve jürimiz tarafından kabul edilmiştir.

JÜRİ ÜYELERİ **İMZA**

Tez Danışmanı:

Prof. Dr. İsmail Ermağan .....

Kurumu: İstanbul Medeniyet Üniversitesi

Üyeler:

Doç. Dr. Fatih Bayram .....

Kurumu: İstanbul Medeniyet Üniversitesi

Dr. Öğr. Üyesi Mehmet Ali Ertürk .....

Kurumu: İstanbul Üniversitesi

Tez Savunma Tarihi: 28 / 06 / 2024

BEYANLAR

Yazım ve Kaynak Gösterme Kılavuzu Beyanı

Danışmanlığımda yazılan bu tezin APA yazım ve kaynak gösterme kılavuzunda belirtilen kurallara uygun olarak yapılandırıldığı ve bu kılavuzun metin içi kaynak gösterme standartlarının bu tezde tutarlı olarak uygulandığı tarafımdan incelenerek teyit edilmiştir.

İmza

Prof. Dr. İsmail Ermağan

Etik İlkelere Sadakat Beyanı

Hazırladığım bu tezin tamamen kendi çalışmam olduğunu, akademik ve etik kuralları gözeterek çalıştığımı ve her alıntıya kaynak gösterdiğimi beyan ederim.

İmza

Burak Eskici

ÖZET

Siber Güvenlik Politikalarında Eğitim Ve Türkiye'nin Siber Güvenlik Eğitimi Politikası

Eskici, Burak

Yüksek Lisans Tezi, Uluslararası İlişkiler Anabilim Dalı,
Danışman: Prof. Dr. İsmail Ermağan
Eşdanışman Doç. Dr. Muhammed Ali Aydın
Haziran, 2024

Bilim 2.0 döneminin başladığı 2000'lerden sonra, internetin gelişimiyle bireyler, şirketler ve devletler siber uzayda büyük tehditlerle karşılaşmaktadır. Siber uzay, kara, hava, deniz ve uzayın ötesinde yeni bir boyut olarak güvenlik çalışmalarında önemli bir yer tutar. Bu tez çalışması, dünyadaki ve Türkiye'deki siber güvenlik eğitimini mercek altına alarak incelemektedir.

Türkiye'nin siber güvenlik alanında önemli yatırımlar yapmasına rağmen hem saldırıya uğrayan hem de saldırı gerçekleştiren ülkeler arasında üst sıralarda yer aldığını ve bu anlamda bireysel düzeyde siber güvenlik eğitiminin öneminin yeterince anlaşılamadığı ve bu alanda gereken eğitim seferberliğinin tam anlamıyla gerçekleştirilemediği anlaşılmaktadır.

Devlet, siber güvenlik politikaları geliştirme arayışında olup bu alanda ciddi gelişmeler kaydetmiştir. Özellikle siber güvenlik strateji belgelerinin yayınlanmasıyla önemli adımlar atılmıştır. Şirketler de siber güvenlik uzmanları istihdam ederek, devlet politikalarına ve uluslararası gereklere uyum sağlamaya çalışmaktadır.

Bu çalışma, Türkiye'deki siber güvenlik eğitimine dair doküman analizi yaparak çözüm önerileri sunmaktadır. İnsan faktörü siber güvenlikte en zayıf halka konumundadır dolayısıyla siber güvenlik eğitimi politikalarının doğru ve etkili şekilde oluşturulması elzemdir. Bireylerin siber güvenliğin kritik önemini içselleştireceği bir eğitimle donatılması gerekmektedir. Bu

bağlamda, siber güvenlik eğitiminin mevcut durumu ve olması gereken seviyeye ışık tutmak amacıyla önemli bulgular ortaya konulmuştur. Doküman analizinin yanı sıra, siber güvenlik eğitiminin nasıl geliştirilebileceğine dair öneriler de sunulmuştur.

Anahtar Kelimeler: Siber Güvenlik, Bilim 2.0, Siber Güvenlik Politikası, Siber Güvenlik Eğitimi, Siber Güvenlik Stratejileri, Ulusal Politikalar, Siber Güvenlik Eğitimi Politikası, Siber Güvenlikte Birey Boyutu

ABSTRACT

Education in Cyber Security Policies and Cyber Security Education Policies of Türkiye

Eskici, Burak

Master's Thesis, Depratment of International Relations

Supervisor: Prof. Dr. İsmail Ermağan

Cosupervisor: Assoc. Prof. Dr. Muhammed Ali Aydın

June, 2024

Since the onset of the Science 2.0 era in the 2000s, the development of the internet has exposed individuals, companies, and governments to significant threats in cyberspace. Cyberspace, as a new dimension beyond land, air, sea, and space, holds a crucial place in security studies. This thesis examines cybersecurity education worldwide and in Türkiye.

Despite Türkiye's significant investments in cybersecurity, Türkiye remains among the top countries both attacked and attacking. This indicates a lack of understanding of the importance of individual-level cybersecurity education and an incomplete mobilization of necessary educational efforts in this field.

The government has made considerable progress in developing cybersecurity policies, especially in the publication of cybersecurity strategy documents. Companies are also striving to comply with state policies and international requirements by employing cybersecurity experts.

This study provides an analysis of documents related to cybersecurity education in Türkiye and offers solutions. The human factor is the weakest link in cybersecurity, making the formation of accurate and effective cybersecurity education policies essential. Individuals need to be equipped with an education that internalizes the critical importance of cybersecurity. In this context, the study presents significant findings to illuminate the current state and the desired level of cybersecurity education.

In addition to document analysis, the study offers suggestions on how to improve cybersecurity education.

Keywords: Cybersecurity, Science 2.0, Cybersecurity Policy, Cybersecurity Education, Cybersecurity Strategies, National Policies, Cybersecurity Education Policy, Individual Dimension in Cybersecurity

ÖNSÖZ

Bu çalışma öğretmenlik meslek aşkı ile akademik alan arasında kalan ve her seferinde mesleğini ve öğrencilerini kariyerinin önünde tuttuğu için birçok öğrencisine yetişebilmiş ama kendi kariyer ilerlemesinde geç kalmış bir hayat boyu öğrencinin; hayatının, ülkesinin ve teknolojik evrimin birçok basamağını barındıracak kadar uzun bir sürede ne vazgeçebildiği ne de tam bir sebatla neticeye erdiremediği uzun bir sürecin sonunda tamamlanabilmiştir.

Bu süreçte tüm maddi manevi mazeretlerimi anlayışla karşılayarak her seferinde bana akademik olarak dikey ilerlemeyi yakıştıran ve beni uzun yıllar sabırla taşıyan Danışman Hocam Prof. Dr. İsmail ERMAĞAN'a, aynı şekilde beni akademik anlamda olduğumdan daha ilerde değerlendirip cesaretlendiren ve tezimde son tamamlama girişimimde en büyük destekçim olan Eşdanışman Hocam Doç. Dr. Muhammed Ali AYDIN'a, tez savunma sürecimde mesailerini harcayan, mütevazı ve yapıcı tutumlarıyla tezimin iyileştirilmesinde katkılar sunan jüri üyesi Hocalarım Doç. Dr. Fatih BAYRAM'a ve Dr. Öğretim Üyesi Mehmet Ali ERTÜRK'e, uzayan süreçte her zaman yapıcı ve anlayışlı yaklaşan ve çözüm odaklı çalışan lisansüstü eğitim enstitüsünün değerli çalışanlarına, hayatıma vesile olmuş ve bu yaşımda hala öğrenci velisi olmaktan yorulmamış sevgili anneme ve babama, kendi yüklerine rağmen abisine desteğini hep sürdüren sevgili kardeşim Dr. Burcu'ya sonsuz teşekkürlerimle…

Burak Eskici

İstanbul, 2024

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

AB	Avrupa Birliği
ACCS	Australian Centre for Cyber Security
ACM SIGCSE	Association for Computing Machinery's Special Interest Group on Computer Science Education
ACM ITiCSE	Association for Computing Machinery's Innovation and Technology in Computer Science Education
AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
APT	Advanced Persistent Threat
ARGE	Araştırma Geliştirme
ATASAREN	Atatürk Stratejik Araştırmalar Ve Lisansüstü Eğitim Enstitüsü
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BT	Bilişim Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
BTYD	Bilişim Teknolojileri ve Yazılım Dersi
BÜSİBER	Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi
CBL	Challange Based Learning
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIPM	Certified Information Privacy Manager
CIPP	Certified Information Privacy Professional

CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COP	Child Online Protection
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DsiN	Deutschland sicher im Netz e.V.
EC-Council	International Council of E-Commerce Consultants
ECSM	European Cyber Security Month
EDAM	Ekonomi ve Dış Politika Araştırma Merkezi
ENISA	European Union Agency for Cybersecurity
ERASMUS+	European Region Action Scheme for the Mobility of University Students Plus
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GFCE	Global Forum on Cyber Expertise
IAPP	International Association of Privacy Professionals
IBM	International Business Machines Corporation
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IGF	Internet Governance Forum
INSS	Institute for National Security Studies
IOT	Internet of Things

IPS	Intrusion Prevention System
ISC²	International Information System Security Certification Consortium
ISEA	Information Security Education and Awareness
ISO	Uluslararası Standartlar Organizasyonu
ISOC	Internet Society
IT	Information Technology
ITU	International Telecommunication Union
İTÜ	İstanbul Teknik Üniversitesi
IoE	Internet of Everything
IoT	Internet of Things
KAS	Konrad Adenauer Stiftung
MEITY	Ministry of Electronics and Information Technology (India)
MEB	Milli Eğitim Bakanlığı
MİT	Milli İstihbarat Teşkilatı
MTAL	Mesleki ve Teknik Anadolu Lisesi
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NCIA	NATO Communications and Information Agency
NICE	National Initiative for Cybersecurity Education
NIELIT	National Institute of Electronics & Information Technology
NIST	National Institute of Standards and Technology

OECD	Organisation for Economic Co-operation and Development
OTA	Online Güvenilirlik İttifakı
RTÜK	Radyo ve Televizyon Üst Kurulu
SAHAB	Sanal Hava Boşluğu
SANS	SysAdmin, Audit, Network, and Security Institute
SGEP	Siber Güvenlik Eğitim Portalı
SIC	Security Intelligence Center
SIEM	Security Information and Event Management
SSB	Savunma Sanayii Başkanlığı
STK	Sivil Toplum Kuruluşu
STM	Savunma Teknolojileri Mühendislik ve Ticaret Anonim Şirketi
TBD	Türkiye Bilişim Derneği
TSGK	Türkiye Siber Güvenlik Kümelenmesi
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UNODC	United Nations Office on Drugs and Crime
US	United States
USCYBERCOM	United States Cyber Command
USMA	United States Military Academy
USOM	Ulusal Siber Olaylara Müdahale Merkezi
YÖK	Yüksek Öğretim Kurumu

1. GİRİŞ

Son elli yıla damgasını vuran en önemli gelişme alanı konumunda bulunan bilgi ve iletişim teknolojilerinin, günümüzde küresel anlamda ne derece riskler ve avantajlar oluşturabilmekte olduğunu özellikle son on yılda yaşanan vakalardan idrak edebilmek mümkündür. Bilgi ve iletişim teknolojilerindeki insanlık tarihinin son elli yılında hız kesmeyen, sürekli yenilenen ve bir önceki gelişmeyi tarihin raflarına kaldıran acımasız, son derecede hızlı ve insanların toplumsal yaşamlarının her alanına etki eden gelişmelerin bugün geldiği nokta ve gelecekteki ön görülemez gidişatı heyecanlandırıcı ancak bir o kadar da ürkütücüdür.

İnsanların değerleri ve yaşam alanları küreselleşmeyle daha da iç içe geçmekteyken bir taraftan da bilgi ve iletişim teknolojilerindeki bu muazzam gelişim süreci insanlara önce uzay çalışmaları neticesinde dünyanın dışında bir fiziki ortama ulaşma imkânı tanımıştır. Günümüzdeyse gelişim süreci öyle bir noktaya gelmiştir ki; milyarlarca insanın yaşamlarının ciddi bir bölümünü fiziki dünyanın dışında, bilgi ve iletişim teknolojileri marifetiyle oluşturulan sanal bir uzayda yaşamaya başladıkları görülmektedir.

Uluslararası ilişkiler, özellikle 20. yüzyılın ikinci yarısında önemli değişimlere uğramaya başlamıştır. Bu dönemde, devletleri, bireyleri ve toplumları derinden etkileyen yeni teknoloji kaynakları ortaya çıkmıştır. Bunlardan en önemlisi, günümüz bilgisayarının ilk elektronik atalarının geliştirilmesi ve yapay zekâ teknolojilerinin öncüllerinin ortaya çıkmaya başlamalarıdır.

1970'lerde ve özellikle 1990'larda internetin keşfi ile dünya hızla dijitalleşmeye doğru evrilmiştir. Dijitalleşen dünya, bazılarının siber uzay, bazılarının ise dijital uzay olarak adlandırdığı yeni bir kavramı beraberinde getirmiştir. Bu bağlamda, devletler altyapılarını bu yeni gerçekliğe uyum sağlayacak şekilde düzenlemişlerdir.

Dünyada hem gelişmiş hem de gelişmemiş devletler bulunmaktadır. Ancak bu yeni teknolojiye sahip olan, onu etkin bir şekilde kullanan ve altyapısını üreten devletler, interneti okyanus altı kablolar üzerinden uzaya taşımışlardır. Günümüzde, bir çanta boyutundan nano boyutlara kadar küçültülen bilgisayar

sistemleri ve uydu filoları sayesinde, küresel erişim sağlanmakta ve yerel otoritelerin zaman zaman çaresiz kaldığı bir durum ortaya çıkmaktadır. Devletler bu süreçte hem avantajlar hem de dezavantajlar yaşamışlardır.

Gelinen bu noktada, şirketlerin, devlet kurumlarının ve bireylerin hesaplarının her biri, özellikle 2000'li yıllardan sonra hızla ilerleyen dijitalleşme dünyasında çeşitli risklerle karşı karşıya kalmıştır. Devletin kozmik odalarındaki veya hukuk dairelerindeki bir belgenin sanal ortama düşmesi, onun çalınabilir ve kullanılabilir hale gelmesine neden olmuştur. Bu durum, uluslararası bağlamda dijitalleşmenin, yeni çığır açan teknolojilerden biri olarak uluslararası ilişkilere olan etkisini artırmış ve bireylerin, devletlerin ve şirketlerin güvenliğini ve gelişmesini etkileyen önemli bir kriter haline gelmiştir.

21. yüzyılın başından itibaren uluslararası ilişkiler disiplini, teknoloji ile olan derin ve karmaşık bağını giderek daha fazla kavramaya başlamıştır. Bilim 2.0 ile birlikte bilgi paylaşımı ve iş birliği, küresel ağlar aracılığıyla daha erişilebilir hale gelmiştir böylece uluslararası iş birliği ve rekabet yeni boyutlar kazanmıştır. Endüstri 4.0, üretim süreçlerinde dijital dönüşümü ifade ederken, küresel tedarik zincirleri ve ekonomik ilişkilerde köklü değişikliklere yol açmıştır. Yapay zekâ ve kuantum teknolojileri gibi inovatif kavramlar, yalnızca teknolojik ilerlemeyi değil, aynı zamanda ulusal güvenlik politikalarını ve küresel güç dengelerini de şekillendirmektedir. Bu bağlamda, siber güvenlik politikaları, eğitim yoluyla güçlendirilmiş yetkin insan kaynağına duyulan ihtiyacı ortaya koymaktadır. Türkiye'nin siber güvenlik eğitim politikaları, uluslararası arenada rekabet edebilir bir teknoloji ve bilgi toplumu oluşturma hedefiyle şekillendirilmiştir (Ermağan, 2022; Ermağan, 2024).

Siber uzay ülkemizde henüz mahiyeti fark edilmemiş belki de henüz sırasına kavuşamayacak kadar öncüllerinin gerisinde kalmış bir alan olsa da son yıllarda özellikle de sosyal medyanın toplumumuzda kontrolsüzce yaygınlaşmasının neticesinde kritik devlet kurumlarımızın geç de olsa el attığı bir alan durumundadır. Nihayet 2012 yılında resmî gazetede yayınlanan bir karar ile ulusal stratejimizde siber güvenlik konularının önemli yeri ve yapılması gerekenlerin planlanması konusundaki ciddiyet beyan edilmiş ve kayıt altına alınmıştır (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 2012). Bu önemli adımın

ardından Türkiye 2013 yılında "Ulusal Siber Güvenlik Stratejisi" ni oluşturmuş ve bunu bir eylem planı ile birlikte ilan etmiştir (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2013). Bu belge, yasal düzenlemelerin hayata geçirilmesi, adli süreçlerin desteklenmesi için gerekli çalışmaların yürütülmesi, ulusal siber olaylara müdahale organizasyonunun kurulması, ulusal siber güvenlik altyapısının güçlendirilmesi, siber güvenlik alanında nitelikli insan kaynağının yetiştirilmesi ve farkındalık faaliyetlerinin yürütülmesi, yerli teknolojilerin geliştirilmesi ve ulusal güvenlik mekanizmalarının kapsamının genişletilmesi gibi stratejik siber güvenlik eylemlerini içermektedir

Ülkemizde uzun bir zaman zarfında siber saldırılar sadece siber suç kapsamında algılandı ve önemli güvenlik birimlerimize yapılan saldırılar terörle mücadele kapsamında değerlendirildi. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) öncülüğünde devlet kurumlarında siber güvenlik bilincinin artması amaçlandı (Bıçakçı, 2013, s. 45). Son on yıldaki önemli gelişmeler siber güvenlik alanında adımların geç de olsa atılmasını sağladı.

Ülkemizde son on yılda siber güvenlik, siber uzaydaki risklerin farkındalığı ve önlemlerin alınması yolunda ciddi adımların atılması süreci artan bir ivmeyle devam etmektedir. Bölgemizdeki karışıklıkların fitilinin ateşlenmekte olduğu en önemli ortamlardan birinin siber uzayın bir alanı olan sosyal medyada gelişmekte olduğuna dikkat etmek gerekmektedir. Ülkemizde siber güvenliğin sağlanmasına yönelik eylem planında her ne kadar eğitim faaliyetlerinden söz ediliyor olsa da bu hususta sıra henüz kamu kurum ve kuruluşlarındaki kritik personellerin eğitiminden okullardaki çocuklarımızın eğitimine ve bilinçlendirilmesine gelememiştir. Bilişim eğitimindeki bu eksikliklerinin ülkemizde ciddi istihbarat açıkları doğuracağı ve özellikle genç nüfusumuzun siber uzayda başıboş denebilecek bir halde günlük yaşamlarının ciddi bir bölümünü harcamakta olmaları söz konusu riskin olasılığını ve olası tahribini ortaya koymaktadır.

Siber güvenlik açıklarının ortaya çıkması, siber güvenlik politikalarının dünya genelinde diğer devletler, şirketler, kurumlar ve bireyler tarafından organize edilmesi, anlaşılması, öğrenilmesi ve eğitilmesi açılarından kritik ve stratejik bir konuma gelmesini sağlamıştır. Bu tez, bu bağlamda siber güvenlik

eğitiminin dünya literatürüne bir bakış sunarak, Türkiye'deki siber güvenlik eğitiminin durumunu irdelemeyi amaçlamaktadır. Tezin başlıca araştırma soruları şunlardır:

1. Dünyada siber güvenlik politikalarının önemi nedir?
2. Kritik öneme sahip başat devletlerde siber güvenlik eğitimi nasıl gerçekleştirilmektedir?
3. Türkiye'de siber güvenlik eğitiminde hangi sorunlarla karşılaşılmaktadır?
4. Türkiye'de siber güvenlik eğitim politikaları dünya ölçeğinde nerede konumlanmaktadır?
5. Türkiye'nin siber güvenlik eğitimi nasıl gerçekleştirilmektedir?

Bu sorular çerçevesinde tez, araştırma sorularına dayanan belirli hipotezleri test etmeyi amaçlamaktadır:

- Dünya genelinde internet ve sosyal medyanın, yani dijitalleşmenin devasa boyutlara ulaştığı bu dönemde, siber güvenlik politikalarının siber uzaydaki risklere karşı kritik önemde olduğu görülmektedir. Siber güvenlik eğitimi, bu risklerin giderilmesine yönelik önemli bir faktördür.
- Türkiye, başından itibaren siber güvenliğin öneminin farkında olarak çeşitli politikalar üretmiştir. Ancak, Türkiye'deki insan kaynağı ve tam teşekküllü eğitim konularında, teoride güçlü olmasına rağmen pratikte bazı eksiklikler bulunmaktadır.
- Dünya genelinde North Atlantic Treaty Organization (NATO), Organisation for Economic Co-operation and Development (OECD) ve Dünya Bankası gibi uluslararası kurumlar; siber güvenlik politikalarında eğitimi gündeme alarak siber güvenlik eğitiminin önemine yıllık raporlarında yer vermektedirler.
- Türkiye hem en çok siber saldırıya uğrayan hem de en çok saldırı gerçekleştiren ilk 10 ülke arasında yer almaktadır. Bu durum, Türkiye'nin potansiyelini ve karşı karşıya olduğu riskleri göstermektedir.

Literatür taramalarında siber güvenlik eğitimi politikası üzerine kapsamlı bir çalışma bulunmadığı anlaşılmaktadır. Yerel literatürde karşılaşılan en önemli kaynakların daha ziyade siber güvenliğin uluslararası ilişkiler disiplinindeki araştırmacıların çoğunlukla siber güvenlik konusunda teknik hususlardan ziyade siber güvenlik politikaları ve stratejileri üzerinde, dünya güvenliği, mukayeseli durumlar ve ulusal güvenlik gibi başlıklarda çalışmalar şeklinde yoğunlaştığı görülmüştür.

Türkiye, dijital dönüşümün getirdiği risklere karşı önlem almak amacıyla çeşitli düzenlemeler yapmıştır. Bu düzenlemeler, özellikle kamu ve özel sektörün iş birliği ile siber güvenlik kapasitelerini artırmayı hedeflemektedir. Türkiye'nin siber güvenlik politikaları, ulusal güvenliği sağlama ve insan haklarını koruma arasında bir denge kurmayı amaçlamaktadır (Akyeşilmen, 2016a; Özker, 2022).

Akyeşilmen (2019), siber çatışmaların uluslararası güvenlik politikalarına etkisini incelemiş ve siber güvenliğin sadece teknik bir mesele değil, aynı zamanda politik bir mesele olduğunu vurgulamıştır. Bu bağlamda, siber güvenlik eğitimi, uluslararası çatışmaların ve siber savaşların önlenmesinde kritik bir rol oynayabilir. Özellikle, uluslararası iş birliği ve bilgi paylaşımı yoluyla siber güvenlik farkındalığının artırılması, küresel güvenlik politikalarına katkıda bulunacağı ifade edilmektedir (Akyeşilmen, 2019). Özellikle, okullarda ve yükseköğretim kurumlarında siber güvenlik eğitiminin müfredata dâhil edilmesi, genç nesillerin siber tehditlere karşı daha bilinçli ve donanımlı olmasını sağlayacağı ortaya konulmaktadır (Akyeşilmen, 2016b). Türkiye'nin küresel siber güvenlik arenasındaki stratejileri, ülkenin siber güvenlik eğitimine yönelik politikalarının uluslararası standartlara uyum sağlamada önemli bir rol oynamaktadır ve Türkiye'nin siber güvenlik politikaları, siber tehditlere karşı koymanın yanı sıra uluslararası iş birliğini güçlendirmeyi de hedeflemektedir (Akyeşilmen, 2022).

Türkiye'de siber güvenlik eğitimi, özellikle 2010'lu yıllardan itibaren büyük önem kazanmıştır. Bu dönemde çeşitli ulusal strateji belgeleri ve eylem planları hazırlanmış, bu planlarda siber güvenlik eğitiminin kritik önemi vurgulanmıştır (Darıcılı, 2019). Siber güvenlik eğitimi, hem kurumsal hem de bireysel düzeyde farkındalık yaratmayı ve teknik bilgi birikimini artırmayı

hedeflemektedir. Eğitim programları, okullarda müfredatın bir parçası haline getirilmiş ve bu konuda çeşitli eğitim materyalleri ve araçlar geliştirilmiştir (Darıcılı, 2019).

Alanda yapılan literatür taramaları, çocuklar için kapsamlı bir dizi öneri veya siber güvenlik eğitim programı sağlamaya yönelik kapsamlı bir girişimin bulunmadığını ortaya koymaktadır. Var olan literatürde bireylere yönelik siber güvenlik eğitiminin içeriği ve sunumuna ilişkin kaynaklar, tutarlı bir dizi derleme şeklinde düzenlenmeye çalışılmaktadır. Ayrıca, küresel bağlamda etkili müfredat ortaya konulmasına yönelik anlamlı olabilecek bazı sorunlu boşluklarla ve kapsamlı varsayımlarla da karşılaşılmaktadır.

Bugüne kadar, siber güvenlik eğitimi konusunda araştırmacılar çeşitli siber güvenlik risklerini ve farkındalık artırıcı yaklaşımları araştıran bir dizi sistematik literatür taramaları yapmıştır (Zhang-Kennedy ve Chiasson, 2020; Rahman ve ark., 2020; Švábenský ve ark., 2020; Quayyum, Cruzes ve Jaccheri, 2021).

Quayyum ve ark. (2021) öğretim için yedi ana yöntemi; eğitim, oyun tabanlı öğrenme, müdahale, oyunlaştırma, uyarı, aile evinde siber güvenliğin müzakere edilmesi ve mobil uygulama şeklinde ortaya koymaktadır. Okullara siber güvenlik müfredatının yapılması, bu araştırmada eğitim kategorisi altında belirlenen farkındalık yaratma yaklaşımlarından biridir. Ancak müfredatta yer alması gereken içeriğe ilişkin bir tartışma yoktur (Quayyum, Cruzes ve Jaccheri, 2021).

Benzer şekilde, Zhang-Kennedy ve Chiasson (2020), siber güvenlik farkındalığı ve eğitimi için multimedya araçlarındaki eğilimleri raporlamak amacıyla bir çalışma yürütmüşlerdir. Mevcut eğitim araçlarında kullanılan öğretim tasarımı ilkelerinin analizine çalışmalarında yer vermişlerdir. Ancak çalışmalarının odak noktası, bu araçlar kullanılarak öğretilen içeriklere bakılmaksızın, siber güvenlik farkındalığı ve eğitiminde kullanılacak araçlar üzerinde yoğunlaşılmıştır.

Rahman ve ark. (2020), 2011-2019 yılları arasında yayımlanan makalelerden oluşan bir örnek kullanarak okullarda siber güvenlik eğitiminin önemine ilişkin bir çalışma gerçekleştirmişlerdir. Çalışmaları siber güvenlik eğitiminin neden

önemli olduğuna ve hangi stratejilerin kullanılabileceğine odaklanmıştır. Bu çalışmada da başarılı siber güvenlik eğitiminde hangi içeriğin yer alması gerektiğine dair bir odaklanma veya öneri yoktur.

Švábenský et al. tarafından yürütülen başka bir çalışmada (2019); özellikle siber güvenlik eğitimine odaklanmış ve kapsanacak içeriği değerlendirmiştir. Ancak belirlenen müfredat ve içerikler, bilgisayar eğitimi alanında önde gelen mekânlar olan ve ağırlıklı olarak Amerika Birleşik Devletleri'ndeki (ABD) yükseköğretime odaklanan Association for Computing Machinery Special Interest Group on Computer Science Education (ACM SIGCSE) ve Association for Computing Machinery Innovation and Technology in Computer Science Education (ACM ITiCSE) konferanslarında yayımlanan makalelerden alınmıştır. Bu durum, küresel ölçekte çocukları hedef almakta olup, siber güvenlik eğitim içeriğini belirlemede yetersizdir.

Çocuklara yönelik siber güvenlik eğitimi ile ilgili literatürde belirlenen temalar, ne öğretilecek, nasıl öğretilecek ve kime öğretilmelidir şeklinde tartışılmaktadır. Birinci tema altında literatürde yer alan siber güvenlik içeriklerine ilişkin tartışmalar gruplandırılmıştır. Siber güvenlik eğitiminde yararlı olduğu iddia edilen bilgisayar tabanlı ve sınıf tabanlı eğitimler, nasıl öğretilir teması altında literatürde ele alınmaktadır. Son olarak, siber güvenlik eğitiminden sorumlu tutulan taraflar, kimin öğretmesi gerektiği teması altında gruplandırılmıştır.

Literatürde, siber güvenlik eğitiminin uygulamaları konusunda çeşitlilik mevcuttur. Bazı araştırmalar, siber güvenlik eğitiminde kolaylaştırıcı olarak kullanılabilecek teknik çözümleri ele alırken, bazıları ise siber güvenlik kavramlarının öğretiminde etkili olabilecek sosyal veya eğitsel yaklaşımlar önermektedir. Bu nedenle çalışma boyunca bu iki alt tema için farklı kodlar oluşturulmuştur. Literatürde, araştırmacıların sıklıkla tartıştığı üç ana unsur açısından; kimlerin eğitimde etkin rolleri olduğu konusunda bir fikir birliğine varıldığını söylemek tam mümkün olmasa da bu unsurlar şunlardır: Bunlar; öğretmenler, ebeveynler ve devlet kurumları olarak ortaya konulmaktadır.

İlk iki temada çeşitlilik oldukça yüksektir. Örneğin, ne öğretileceğine ilişkin olarak, bazı çalışmalar (örn., Borowski, Diethelm ve Wilken, 2016;

Hartikainen, Livari ve Kinnula, 2019; Lavie-Dinur, Aharoni ve Karniel, 2021) çocuklarla kendi algıladıkları bilgi boşluklarının nerede olduğunu ve dolayısıyla hangi içeriğin öğretilmesi gerektiğini değerlendirmek için atölye çalışmaları veya anketler gibi "aşağıdan yukarıya" yaklaşımlar kullanmıştır. Bu bölümde atıfta bulunulan diğer çalışmalar (örneğin, von Solms ve von Solms, 2014; Rodríguez-de-Dios ve Igartua, 2016), uzmanların öğrencilerin siber güvenlik açısından bilmesi gerektiğini düşündükleri perspektiften gelen yukarıdan aşağıya yaklaşımlara dayalı daha stratejik tavsiyeler oluşturmuştur. Bu iki yaklaşım çoğu zaman en çok hangi içeriğe ihtiyaç duyulduğu konusunda farklı değerlendirmelerle sonuçlanır. Dolayısıyla bu çalışmalar bu bölümde ayrı ayrı ele alınmaktadır.

Son olarak, literatürde eğitim programlarına liderlik etmede anahtar rol oynayan etkili hükümet girişimlerinin önemi vurgulanmıştır (von Solms ve von Solms, 2014; Wang et al. , 2019). S. von Solms ve R. von Solms (2014) hükümetlerin siber güvenliği destekleyecek yapılar geliştirmedeki rolünü vurgulamışlardır. Siber güvenlik kültürünü teşvik etmek amacıyla yaptıkları çalışmada siber güvenlik girişimlerinin araştırılmasına ve eğitimine yönelik destek ve finansman önerilmiştir. Siber güvenlik standartlarına uygunluğun teşvik edilmesi de belirtilen başka bir hususdu. Siber güvenlik eğitimi için sağlıklı, uygar ve düzenli bir ağ ortamının oluşturulmasında işlevsel bir role sahip olmak, Wang et al. (2019) tarafından devlet kurumlarına verilen bir diğer sorumluluktur.

Tüm bu literatür verilerinin sonucunda bu çalışmanın amacı siber güvenlik politikalarını ve eğitimini birlikte incelemesi açısından literatüre katkı sağlamasıdır. Bu tez, siber güvenlik politikalarında eğitimin önemini ve Türkiye'nin bu alandaki mevcut durumunu ortaya koyarak, gelecekteki çalışmalar ve politikalar için önemli bir kaynak olmayı amaçlamaktadır.

Bu çalışma, siber güvenlik politikalarında eğitimin rolünü ve Türkiye'nin siber güvenlik eğitimi politikasını kapsamlı bir şekilde incelemektedir. İlk bölümde, siber güvenlik, siber tehditler ve siber saldırılar gibi temel kavramlar tanımlanarak kavramsal bir çerçeve oluşturulmaktadır. İkinci bölümde, siber güvenlik politikalarının önemi ve bu politikaların oluşturulmasında eğitimin kritik rolü ele alınmaktadır. Siber güvenlik eğitimi, bireylerin ve kurumların

siber tehditlere karşı bilinçlendirilmesi ve bu tehditlere karşı koyma yeteneklerinin artırılması amacıyla düzenlenen programları kapsamaktadır. Çalışmada, küresel ölçekte siber güvenlik eğitiminin nasıl yapılandırıldığı, başat ülkelerdeki uygulamalar ve bu eğitim politikalarının etkinliği detaylı olarak incelenmektedir.

Türkiye özelinde ise, ülkenin siber güvenlik stratejileri ve bu stratejiler içinde eğitimin yeri detaylı bir şekilde değerlendirilmektedir. Türkiye'de siber güvenlik eğitimi alanında yapılan çalışmalar, mevcut eğitim programları ve bu programların etkinliği analiz edilmektedir. Ayrıca, Türkiye'nin siber güvenlik eğitimine dair ulusal politikaları, ilgili mevzuatlar ve uygulamalar kapsamlı bir şekilde gözden geçirilmektedir. Bu bağlamda, Türkiye'nin siber güvenlik eğitim politikasının güçlü ve zayıf yönleri tartışılmakta ve bu alanda gelecekte yapılması gerekenler hakkında öneriler sunulmaktadır.

Sonuç ve değerlendirme bölümünde, Türkiye'nin siber güvenlik eğitimi politikasının mevcut durumu ve bu politikaların gelişim potansiyeli ele alınmaktadır. Çalışmanın sonucunda, eğitimin siber güvenlik alanında kritik bir bileşen olduğu vurgulanmakta ve Türkiye'nin bu alandaki performansının iyileştirilmesi için öneriler sunulmaktadır.

2. KAVRAMSAL ÇERÇEVE

Aslında bir ön ek olan *siber* sözcüğünün temeli 1948 yılında Novert Weiner'ın "*hayvanlarda ve makinelerde iletişim ve kontrol bilimi*" olarak ifade ettiği *sibernetik* kavramından gelmektedir (Çakmak & Altunok, 2009). Çalışmamızın başlığında olduğu gibi ilgili alandaki özellikle bilişim teknolojilerinde birçok tanımlamada anlam kazanan ve bir sıfat olarak birçok sözcüğü V. boyuta taşıyan siber sözcüğü ile anılan temel tanımlara özellikle de siber güvenlik eğitimi ve siber güvenlik politikalarına dair temel kavramlara bu bölümde yer verilmektedir.

2.1. SİBER GÜVENLİĞE DAİR TEMEL KAVRAMLAR

2.1.1. Siber Uzay

Sibernetik ve uzayı birlikte ilk olarak William Gibson kısa bir öyküde 1982 yılında yer vermiştir. Yine aynı yazar siber uzay kavramını 1984 yılında *Neuromancer* adlı romanında "*milyarlarca kullanıcının deneyimlediği sanrı"* olarak açıklamıştır (Singer & Friedman, 2015). Gizemli bir hava uyandıran "siber" sözcüğü ve uzayla oluşan bu tamlama farklı kurumlarca defalarca farklı tanımlamaları yapılmış hatta bazı kurumların farklı yıllarda farklı tanımlamalar ortaya koydukları tek bir tanımlamada mutabakatı sağlanamamış bir kavramdır. Singer ve Friedman (2015) bu tanımlama zorluğunu kavramın genişleyen küresel bir doğasının olmasının yanı sıra mütevazi şekilde başlayan siber uzay mefhumunun şu an tanınmaz hale geldiğiyle muhtemelen hayali dahi zorlaşan bir mahiyete bürünmesiyle açıklamaktadırlar (Singer & Friedman, 2015, s. 28).

2003 yılında Beyaz Saray tarafından siber uzay; "*Siber alan, kritik alt yapılarımızın çalışmasını sağlayan, birbirine bağlı yüz binlerce bilgisayar, sunucu, yönlendirici, anahtar ve fiber optik kablolardan oluşur*" şeklinde tanımlanmıştır (The White House, 2003).

2006 yılında ABD Savunma Bakanlığı siber uzayı; "*İletişim ağı ile birbirine bağlanan sistemlerde, veri saklama, değiştirme ve iletme amacıyla elektronik ve elektromanyetik spektrumun kullanıldığı alandır.*" şeklinde tanımlamıştır. Yine aynı kurum 4 yıl sonra 2010 yılında tanımı genişleterek Singer ve

Friedman'nın tanımlama zorluğuna dair açıklamasını destekler şekilde; "*İnternet, iletişim ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, birbirine bağımlı ağların oluşturduğu bilgi ortamındaki küresel bir alandır.*" olarak güncellemiştir (Department of Defense, 2010).

2011 yılında NATO siber uzay kavramını *"Bilgisayarlar ve bilgisayar ağlarının ortaya çıkardığı; insanlar ve bilgisayar ağlarının bir arada bulunduğu ve çevrim içi faaliyetlerin tüm yönlerini içeren sayısal bir dünyadır."* şeklinde tanımlarken AB Komisyonu: *"Dünya çapında kişisel bilgisayarların elektronik verilerinin dolaştığı sanal ortamdır."* şeklinde tanımlamıştır (Çifci, 2013, s. 4).

Ulusal Siber Güvenlik Stratejisi (2016-2019) belgesine göre siber uzay, dünya genelinde ve uzayda yayılmış bilgi ve iletişim teknolojileri ile bunları birbirine bağlayan ağlar veya bağımsız bilgi sistemlerinden oluşan dijital bir ortam olarak tanımlanmaktadır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016).

Siber uzayın temel özelliklerini Çifci (2013, s. 8) sekiz başlıkta açıklamıştır:

- Diğer harekât boyutlarından farklı olarak büyük ölçüde özel sektörün elinde olan insan ürünü bir alandır.
- Birbirlerine bağlı ya da bağımsız bilgi ve iletişim teknolojileri sistemlerinden ve buralarda işlenen verilerden oluşur.
- Kamu kuruluşlarının, özel şirketlerin veya kişilerin oluşturduğu, sahip olduğu, yönettiği ve işlettiği, dünyanın hemen hemen tümüne yayılan bir alandır.
- Bilgi ve iletişim teknolojileri çerçevesinde teknik mimarilerin, stillerin, işlemlerin, yeni kabiliyetlerin ve yöntemlerin gelişmesiyle değişir.
- Siber uzayda etkileşim, iletim ve iletişim neredeyse ışık hızında gerçekleşir.
- Işık hızına yakın olan harekât kabiliyeti beraberinde ışık hızında tehdit etkisi doğurur.
- Kendisi dışında kalan tüm harekat alanlarında da (kara, hava, deniz, uzay) harekat kabiliyetini mümkün kılar.

- Coğrafi ve siyasi sınırlardan bağımsızdır ve dolayısıyla harekât alanı bağlamında da sınırsızdır.

2.1.2. Siber Güvenlik

Yeni bir harekât alanı olarak savaş sahnesinde yerini alan siber uzay ortamında nasıl ki savaş söz konusuysa elbette bu savaşta savunma ve güvenlik unsurları da olacaktır. En kritik noktalardan başlanmak üzere tüm kurum ve kuruluşlarda, kritik sektörlerde ve tabi ki kişisel kullanıcılarda da sağlanması gereken güvenlik gereksinimleri vardır. Bunların önceliği ve seviyesi önem ve risk durumuna göre farklı olabilir ancak mutlaka siber uzayın tehditlerine karşı güvenli kılınmaları gereklidir. Her ne kadar sınırları ve saldırı kabiliyetleri sınırlı olmasa da siber uzayda güvenlik önlemleri siber uzayın sınırsız karakterine uygun bir şekilde alınmaya devam etmek zorundadır.

Siber uzay kavramında olduğu gibi siber güvenlik açısından da mutabakat sağlanmış net bir tanım daha doğru ifadeyle tek düze bir tanım yoktur. Belli başlı tanımlar şu şekildedir:

International Telecommunication Union (ITU) siber güvenliği "siber çevre, kurumlar ve bireylerin varlıklarını korumak adına kullanılabilecek araçların, politikaların, güvenlik kavramlarının, güvenlik talimatlarının, risk yönetim yaklaşımlarının, eylemlerin, kursların, en iyi örneklerin, güvence ve teknolojilerin toplamı" olarak tanımlamaktadır (Cavelty, 2015).

National Initiative for Cybersecurity Education (NICE) siber güvenliği, "*bilgi ve iletişim sistemleri ile bu sistemlerin içerisinde yer alan bilgilerin herhangi bir zarara, saldırıya ya da yok edilmeye karşı korunduğu, savunulduğu bir faaliyet ya da süreç"* olarak tanımlamaktadır. Söz konusu kurum siber güvenlik tanımını daha da açarak; siber uzaydaki söz konusu olan tüm operasyonları, güvenlik politikalarını, stratejileri, standartları, bütün riskleri, açıkları, caydırıcı boyutu, uluslararası ittifakları, hazırbulunuşluğu, veri geri getirme politikalarını, istihbari, askeri ve diplomasi anlamında alakalı global bilgi ile iletişim altyapılarının güvenliği gibi hususları eklemiştir (Cavelty, 2015).

Tüm bu tanımlardan hareketle özetlemek gerekirse; siber uzayda yer alan tüm unsurların, devlet kurumlarının, özel teşekküllerin, çok ciddi öneme sahip ve

kritik alt yapı diye nitelendirilebilecek tesislerin, bilgi ve iletişim kaynaklarının ve dağıtıcılarının, medya ve basın kuruluşlarının, devletin siber uzayda sunduğu e-devlet kapısı gibi hizmetlerin, ulaşım ve enerji sektörlerinin, her bir kişisel bilgisayar hatta günümüzde her biri bilgisayar özellikleriyle donatılmış mobil cihazların kısacası siber uzaya bağlı her şeyin güvenliği için alınacak her türlü, teknik, sosyal, kültürel, ekonomik ve siyasi tedbirler siber güvenliği teşkil eder.

2.1.3. Siber Saldırı

Siber saldırılar, veriler içeren ağlara, sızdırma, manipüle etmek ve ortadan kaldırmak için gerçekleştirilebilmektedir. Saldırılar, siber uzaydaki bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini tahrip etmeyi amaçlamaktadır (Białoskórski, 2012).

Günümüzde siber saldırılar, yalnızca sistemlere sızma, bilgi çalma, bilgi yerleştirme veya mevcut bilgiyi bozma eylemleriyle sınırlı değildir. Aynı zamanda, bir ülkenin haberleşme, sağlık, bilgi, enerji ve ulaşım sistemleri ile komuta ve kontrol ağlarına zarar verebilecek kadar asimetrik bir harp türü olarak tanımlanmaktadır (Göçoğlu, 2018).

Kritik altyapıları devre dışı bırakmak, yemleme olarak bilinen tuzak içeriklerle veri sızdırmak, çeşitli yazılımlar aracılığıyla sistemlere zarar vermek, sosyal mühendislik teknikleri kullanmak, ağa sızmak, veri çalmak ve değiştirmek gibi yöntemlerle devlet veya ticari kuruluşların internet sitelerini bozmak, sistemdeki gizli bilgileri çalmak, silmek, ifşa etmek veya değiştirmek amacıyla hedef kişi, şirket veya kurumların iletişim altyapılarına veya bilgi sistemlerine yönelik, genellikle önceden yapılan detaylı analizler ve özel çalışmalar sonucunda gerçekleştirilen saldırılar, siber saldırı olarak adlandırılmaktadır (Çakmak & Demir, 2009).

Ulusal Siber Güvenlik Stratejisi'nde bu tanım şu şekildedir: Siber uzayda yer alan bilgi ve iletişim teknolojilerinin gizliliğini, bütünlüğünü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir noktasındaki bireyler veya sistemler tarafından kasıtlı olarak gerçekleştirilen eylemler olarak tanımlanır (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016).

Siber saldırıların niyetleri her ne olursa olsun bağımsız hackerlar, paralı hackerlar, hacktivistler, dahili unsurlar ve ulus devletlerce yapılabileceği belirtilmektedir (Lu & Reeves, 2014).

2.1.4. Siber Terörizm

Siber uzayın doğası düşünüldüğünde, sınırları olmayan ve gizlenmek için çetin doğa koşullarında, dağlarda, mağaralarda füze tehdidi yaşamadan teröristlerin barınabileceği yegâne ortam olduğu gerçeğini ortaya koyuyor. Böyle bir saha elbette terör örgütlerine etkili ve yeni bir eğitim kampına, tedarik zinciri oluşturmaya kadar varabilen imkânlar sağlamaktadır.

Siber terörizm (cyber terrorism), *bilgisayar ağlarını bozmaya yönelik kısıtlı ve geniş kapsamlı eylemler dahil olmak üzere, terör eylemlerinde internet tabanlı saldırıları ve internete bağlı bilgisayarları kullanmaktır*" (Çifci, 2013, s. 6).

Bu tür saldırılar, sınırlı insan kaynağı ile en düşük maliyetle gerçekleştirilebilir ve pek çok hedefi aynı anda etkileyebilir. İletişim olanaklarının gelişmişliğine bağlı olarak, büyük organizasyonlar gerektirmeden yüksek mobilite ve hızlı reaksiyon yeteneği ile karakterize edilir. Asimetrik doğası nedeniyle kaynağında yok edilmesi son derece zordur. Bağlantılarının kanıtlanamaması ve gizliliği açısından bir devlet ile ilişkilendirilmesi neredeyse imkânsızdır. Ayrıca, ulusal ve uluslararası hukuktaki boşluklardan faydalanarak modern savaş tekniği olarak tanımlanabilir (Çitlioğlu, 2008).

Tablo 1 *Siber Terör ile Klasik Terör Arasındaki Farklar (Bayraktar, 2015, s. 50)*

	Klasik Terör	Siber Terör
Kullanılan Araç	Silah, bomba gibi araçlar	Çipler, bilgisayarlar veya bilgi sistemlerinde kullanılan diğer donanımlar, yazılımlar
Amaç	Siyasi rejime ve topluma mesaj vermek için terörizm bir amaç	Yapılan eylemler ile topluma veya devlete zarar verme, siyasi ve sosyal olarak etkilemek için terörizm bir amaç

Tablo 1 *(Devamı)*

	Klasik Terör	Siber Terör
Etki Alanı	Saldırının yapıldığı bölge ya da alan ile sınırlı	Ulusal veya uluslararası boyutlarda etkili
Karşılaşılan Risk	Eylemi gerçekleştiren kişi ya da grup yaşamsal risk altında	Herhangi yaşamsal riski olmadan etkili saldırı
Denetim	Terörü kontrol altında tutma, izlemek ve yok etmek kısmi anlamda mümkün	Siber teröristleri tespit etmek veya yok etmek imkansız
Uygulanacak Ceza	Suçun niteliğine göre uygulanacak ceza belli	Suçun niteliğine göre uygulanacak ceza belli

Siber terörün tanımlarında geleneksel tutum terör eylemlerinin siber uzaya taşınması şeklinde özetlenebilmektedir ancak siber uzayın ileriki bölümlerde ele alınacak olan *sosyal medya* unsuru da düşünüldüğünde siber terörizm artık sadece zarar veren yıkıcı eylemleri siber uzayda gerçekleştirilmesiyle sınırlı kalmayıp propaganda ve militan devşirilmesi anlamında da günümüzde terör faaliyetleri içerisindeki yerini ve önemini ileriye taşımıştır ve taşımaya devam etmektedir.

2.1.5. Siber Casusluk

Siber casusluk, iletişim ağları veya bilgisayarlara kanunlara aykırı şekilde sızarak, kişisel, ekonomik, politik veya askeri avantaj sağlamak amacıyla bireylerden, rakiplerden, gruplardan, ülkelerden veya düşmanlardan izinleri olmadan sırlarını ele geçirme fiilidir (Çifci, 2013, s. 6).

Siber uzaydaki casusluk faaliyetleri insan temelli istihbaratın (HUMINT) yerini alma yolunda çok ciddi bir konuma gelmektedir. Artık ABD'de herhangi bir üstte bulunan komuta kontrol merkezindeki oyun konsoluna benzer kumanda tertibatını kullanan birkaç asker, binlerce kilometre ötedeki insansız hava

aracıyla casusluk faaliyetleri yapabilmekte hatta fiziki müdahale ve imha kabiliyetine sahip olabilmektedir.

Bir başka haliyle siber casusluk, bir ülkenin kritik alt yapılarına sızarak önemli bilgilerin düzenli olarak komuta kontrol merkezine akmasını sağlayabilmektedir. Tabi ki casusluk faaliyetleri ekonomik olarak da prestij olarak da çok ciddi sonuçlar doğurabilmektedir.

Hatırlanmalıdır ki gerek gezi olaylarında gerekse 30 Mart 2024 tarihinde yapılan mahalli idareler seçimleri öncesi sosyal medya adeta bir silaha dönüşmüş, tabi ki bu konuda önlemleri ve yasal alt yapıyı en önemlisi de insanlarımızın bilinçlendirilmesi eğitimlerini ihmal eden yetkililerimiz çok zor durumda kalmışlardır. Önlem almaya çalışmaları uluslararası camiada hemen sansür ve özgürlüklerin kısıtlanması şeklinde yorumlanmış, devletimiz başta ABD ve AB organları tarafından olmak üzere dış dünyanın tepkisiyle karşılaşmıştır.

Artık bakanlar açıklama yapmak için basın mensuplarını toplamaktan ziyade 140 karakterlik paketler halinde twitter mesajlarını paylaşmayı daha çok tercih etmeye başlamışlardır. Dış işleri bakanları arasında mekik diplomasileri artık "ötüş mekikleri" şekline dönüşme yolundadır. Twitter'da paylaşılan bir uluslararası iktisadi veri, dünya borsalarında paniğe hatta krize sebep verebilme potansiyeline sahip hale gelmiştir. Artık özellikle uluslararası tanınırlığı olan makamlardaki insanların gerek gerçek hayattaki gerekse sanal ortamdaki özel yaşamları her an internet ortamına sızdırılabilmektedir. Bu yolla ülkemizde parti liderleri devrilmiş milletvekilleri istifa ettirilmiştir. Ülkenin en mahrem istihbarat toplantısı dahi siber uzayın sınırları yok eden ortamında birileri tarafından ele geçirilmiş ve sosyal medya vasıtasıyla bir anda milyarların önüne serilmiştir. Bu sızıntı yakın siyasi tarihimizde belki de dışişlerimizin ve dış politikamızın aldığı en ciddi istihbari yaralardan birisi olmuştur. Bir anda ülkemizin en üst makamlarındaki insanların sınır ötesi planları herkesin kulağına servis edilmiştir. Bu hadiseyle öyle bir harekât imkânı düşünüşmüş olsa dahi artık herkes bildiğine göre masadan kalkmıştır ve bu da dış politik karar alıcıların seçeneklerine müdahale edilebileceğini, onların güvenilirliklerinin saldırıya uğrayabileceğini herkese göstermiştir.

2.1.6. Siber Savaş

Amerikalı eski Siber Güvenlik Danışmanı Richard Clarke, siber savaşı; *"Siber savaş, bir devlet tarafından, bir devlet adına veya o devleti desteklemek amacıyla başka bir ülkenin bilgisayar veya bilişim ağlarına yetkisiz giriş yaparak veri eklemek, değiştirmek veya bozmak, ya da bilgisayarları, ağ üzerinden cihazları veya bilgisayar sisteminin kontrol ettiği nesneleri kesintiye uğratmak veya onlara hasar vermek amacıyla gerçekleştirilen eylemler bütünüdür"* şeklinde tanımlamaktadır (Clarke & Knake, 2010, s. 119).

Harekât alanları arasında kabiliyetler sınırında önceleri; *kara, hava* ve *deniz* olan, sonradan *uzayın* da eklendiği dörtlüye beşinci bir harekât alanı olarak *siber uzayın* da katılmasıyla savaşlarda yeni ve sınırsız bir cephe açılmıştır.

Siber savaş politik, askeri veya ekonomik gerekçelerle hedef olarak belirlenen düşman ülkeye, sivil, askeri ve hükümete ait siber uzay unsurlarına bilgi ve iletişim teknolojileri unsurları vasıtalarıyla düzenlenen saldırı faaliyetlerinin hayata geçirilmesi olarak da tanımlanmıştır (Yazıcı, 2011).

Libicki'ye göre siber savaş operasyonel ve stratejik olmak üzere iki bölümde incelenmelidir. Operasyonel olan nizami bir savaş sırasında hasmın askeri hedeflerine ve silahlı kuvvetleri ile bağlantılı sivil hedeflerine karşı gerçekleştirilen siber harekât, stratejik olan ise bir devlete ve onu oluşturan topluma karşı özellikle de devletin tutumunu değiştirmek amacıyla gerçekleştirilen siber harekât olarak ifade edilmektedir (Libicki, 2009).

"Clatham House Report" adında 2010 yılında yayınlanmış olan raporda siber savaşların belirgin özellikleri şu şekilde ifade edilmiştir (Clemente, Livingstone, Yorke, & Cornish, 2010):

- Silahlı çatışmaya başvurmadan, siyasi ve stratejik hedeflere ulaşmayı sağlar.
- Küçük ve nispeten önemsiz görünen aktörlere, beklenenden çok daha fazla güç sunar.
- Sahte IP adresleri ve yabancı sunucular kullanarak, kısa süreli anonimlik elde edebilir.
- Geleneksel savaşlardan farklı olarak, kara, deniz, hava ve uzay dışında, siber uzayda, yani beşinci boyutta gerçekleştirilir.

- Konvansiyonel savaşın çatışma ve baskı unsurlarından sonra ortaya çıkmış olsa da, siber savaş fiziksel baskı ve çatışma ortamından uzaktır. Siber savaş ile klasik savaşın karşılaştırmalı temel farklılıklarını ortaya koyan tablo şu şekildedir:

Tablo 2 *Siber Savaş ile Klasik Savaş Kıyaslaması (Çifci, 2013, s. 20)*

Kriterler	*Klasik Savaş*	*Siber Savaş*
Saldırı Kaynağı	*Saldırıların nereden kaynaklandığının bulunması nispeten*	*Saldırının nereden geldiğini tespit etmek çok zordur, hatta bazen imkânsızdır.*
Saldırı Hızı	*Bir füzenin, bir uçağın, tankın veya muharebeye dahil olan başka bir silah/sistem hızı kadardır.*	*Işık hızındadır.*
Etki Alanı	*Çoğunlukla fiziksel alanda etkilidir.*	*Çoğunlukla bilgi ve iletişim sistemleri alanında etkilidir.*
Savaşanlar	*İki veya daha fazla ülkenin silahlı kuvvetleri savaşmaktadır.*	*Bir kişi, bir grup, bir örgüt veya bir devlet savaşabilir.*
Maliyeti	*Kullanılan silah sisteminin maliyetine bağlıdır, pahalıdır.*	*Genelde ucuzdur, bazen bir bilgisayarla etkili olmak mümkündür.*
Silahlar	*Tabanca, top, tüfek, bomba, uçak, gemi, tank, füze, radar vb.*	*Çipler, bilgisayarlar veya bilgi sistemlerinde kullanılan diğer donanımlar, yazılımlar.*
Teknoloji İhtiyacı	*Genelde ileri teknoloji gerektirmektedir.*	*Zaten mevcut olan bilgisayarın kullanılması da mümkün olduğundan çoğunlukla çok yüksek teknik ve teknolojiye ihtiyaç duyulmamaktadır. Ancak, etkili olabilmek için yüksek teknolojinin kullanılması*
Saldırı Belirtileri	*Saldırının farkına varılır.*	*Saldırının farkına varılmayabilir.*
Hasar Tespiti	*Fiziksel etkilerden dolayı, hasar tespiti nispeten kolaydır.*	*Nerede ve ne kadar hasar oluştuğunu tespit etmek çok zordur; çoğu zaman imkânsızdır.*

2.2. SİBER GÜVENLİK POLİTİKALARINA DAİR TEMEL KAVRAMLAR

Siber uzay unsurlarının yani iletişim teknolojileri araçlarının ve ağlarının artık insanların yaşam alanlarının nerdeyse tamamını kapsayacak şekilde yaygınlaşmakta ve artık yaygınlığın ötesinde yoğunlaşmaktadır. Siber uzay

marifetiyle bilgi ve iletişim teknolojileri araçlarının kabiliyetleriyle insanlığa sunulan birçok hizmetler ve sağlanan katkılar olsa da, ne yazık ki bu sistemler çeşitli karmaşık siber tehditlerle karşı karşıyadırlar. İnsanın olduğu her yerde nasıl ki iyi ve kötü yeryüzünün her köşesinde ve tarihin her evresinde söz konusu olmuşsa günümüzde de insanların gerek kişisel kullanımları açısından gerekse tüzel kişiliklerin ve de devletlerin siber uzayda da kötü olarak tanımlanacak her türlü istismara ve saldırılara açık olduğu da kaçınılmaz bir gerçekliktir. Tüm bu tehditlere karşı koyabilecek tedbirler alınması da bir zorunluluktur.

Bu noktada siber uzayın birlikte getirdiği bir zorunluluk olarak da siber güvenlik kavramı devreye girmektedir. Siber güvenlik; ağa bağlı sistemlere ya da ağda dolaşan verilere yetkisiz erişimlerin hatta erişilemese dahi siber uzaydaki erişimin güvenle sürdürülebilirliğini aksatabilecek her türlü insan ya da yapay zekâ kaynaklı saldırıları sezmeye, karşılamaya, durdurmaya ve caydırmaya yönelik çalışmaların tamamını kapsayan karmaşık ve çok katmanlı bir kavramı ifade etmektedir.

Son derece karmaşık ve sınırları çizilemeyen bir risk alanı konumunda olan siber uzayda mahiyetine özel stratejilerin geliştirilmesi ve siber güvenlik politikalarının hayata geçirilmesi gerekmektedir. Uzmanlarca üzerinde iyi çalışılmış ve iyi planlanmış etkili stratejilerin bir bütün olarak politika haline getirilmesi ve bu politikalar doğrultusunda hedefleri ve kuralları anlaşılabilir ve uygulanabilir şekilde açıklayan kılavuzlarla bireylerde davranış ve zihniyet kültürleyebilecek eğitim müfredatlarıyla toplumdaki her birey açısından hayata geçirilmiş bir politikanın sağlanabilmesi gerekmektedir.

Devletler ve büyük verilere hükmeden kuruluşlar açısından durum çok da farklı değildir. Bilgi teknolojisi varlıklarının güvenli kullanımını ve yönetimini tanımlayan uygun güvenlik politikaları belgelerini oluşturmak günümüzde bir zorunluluk haline bürünmüştür. Aksi durumda kaynakların, ekonominin, itibarın hatta bazı kritik alt yapılar söz konusu olduğunda hayatların dahi kaybedilebilmesi tehlikesi ile karşı karşıya kalmak mümkündür.

Siber güvenlik politikasındaki öğeler belirlenirken aşağıdaki hedeflerin sağlanması gerekmektedir (Shafi, 2012):

- **Gizlilik:** Şifreleme ve kimlik doğrulama mekanizmalarıyla korunan veri tabanı yönetim sistemleri ile bilgilerin yetkisiz erişimden korunmasını ve gizliliğini sağlamalıdır.
- **Bütünlük:** Saklanan bilgilerin yetkilendirme mekanizmaları vasıtasıyla değiştirilmesi ya düzenlenmesi açısından korunması gerekmektedir. Bilgilerin doğru ve güvenilir olduğunu garanti etmelidir.
- **Erişilebilirlik (Kullanılabilirlik):** Saklanan bilgilere ve sunulan hizmetlere yetkilendirilen kişilerce yetkileri sınırında erişilebilmesini sağlamalıdır.

Yukarıdaki hedeflere dayanarak, siber güvenlik; kurumların, kuruluşların ve bireylerin varlıklarını siber uzaydaki risklerden korumak amacıyla geliştirilen politikalar, kılavuzlar, güvenlik tedbirleri, risk yönetim stratejileri, eğitim programları ve bilgi ve iletişim teknolojileri unsurları ile bu çerçevede gerçekleştirilen tüm uygulamaları kapsayan bir kavram şeklinde ifade edilebilir (Ünver, Canbay, & Mirzaoğlu, 2009).

Siber uzay, iletişim teknolojilerinin ve ağların yaygınlaşmasıyla insan yaşamının temel bir parçası haline gelmiştir. Ancak, bu yaygınlık siber tehditleri de beraberinde getirmiştir. Siber uzayın karmaşıklığı ve sınırlarının belirsizliği, siber güvenlik politikalarının önemini artırmaktadır.

2.2.1. Siber Güvenlik Politikasının Tanımı ve Önemi

Siber güvenlik politikası, bireylerin, kurumların ve devletlerin kendilerini dijital tehditler ve risklere karşı korumasını sağlar. İnternet ve dijital teknolojilerin yaygınlaşmasıyla birlikte, bilgi güvenliği büyük önem kazanmıştır. Bu alanda yerlileştirilmiş ve millileştirilmiş teknolojilerin geliştirilmesinin artmasıyla ve yine artacak iş birlikleri ile uluslararası rekabet gücüne sahip bir ekosistem oluşturulması hedeflenmektedir (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2023).

2.2.2. Siber Güvenlik Politikasının Uygulanması

Siber güvenlik politikalarının etkin şekilde uygulamaya konması, işletmelerin ve kuruluşların siber tehditler karşısında güvenliklerinin sağlanmasında çok

önemli fark yaratır. Siber güvenlik politikasının etkin şekilde oluşturulması adına izlenebilecek adımlar şu şekildedir: (Ozztech, 2022.)

- **Politika Oluşturma ve Tanımlama**:

Siber güvenlik politikası, tüm çalışanlar için davranışsal ve teknik yönergeler içeren yazılı bir belgedir. Bu politika, bir şirketin veya kuruluşun güvenlik politikaları, prosedürleri, teknolojik önlemleri ve herhangi bir siber güvenlik ihlali söz konusu olduğunda operasyonel karşı önlemleri hakkında bilgi içerir. Politika oluşturulurken, işletmenin türüne, işin doğasına, operasyonel modele ve ölçeğine göre farklı şekiller alabilir.

- **Risk Analizi ve Güvenlik Açıklarının Belirlenmesi**:

Kurumun risklerini anlamak ve güvenlik açıklarını belirlemek önemlidir. Bu, kurumun dijital varlıklarını ve süreçlerini değerlendirmeyi içerir. Sistem sınıflandırması ve gruplandırması yaparak hangi kontrollerin uygulanacağını belirlemek önemlidir.

- **Güvenlik Önlemlerinin Alınması**:

Politika, siber saldırı olasılıklarının sınırlandırılmasını sağlamak için operasyonların ve güvenliğin birlikte çalışmasını destekler. Bilişim Teknolojileri (BT) ekibi, operasyonlar ve işletme yöneticileri, bir saldırı meydana gelirse hangi adımların atılması gerektiğini bilir. Etkili bir siber olay müdahale planı oluşturmak ve bu planı düzenli olarak test etmek önemlidir.

- **Kullanıcı Bilinçlendirmesi ve Eğitimi**:

Kullanıcılar, siber güvenlik politikalarını anlamalı ve uygulamalıdır. Eğitim programları ve farkındalık kampanyaları, kullanıcıların güvenlik konularında bilinçlenmesine yardımcı olur.

2.2.3. Siber Güvenlik Politikalarının Küresel Boyutta Etkisi

Siber güvenlik politikalarının oluşturulması ve de uygulanması, küresel boyutta etkilere sahiptir. Uluslararası iş birliği ve standartların belirlenmesi, siber saldırılara karşı daha etkili bir savunma sağlayabilir. Ancak, farklı ülkelerin kültürel ve yasal farklılıkları nedeniyle, uluslararası bir standart belirlenmesi zorlu bir süreç olabilir (Schreider, 2020).

2.2.4. Siber Güvenlik Politikalarının Geleceği

Siber güvenlik politikalarının geleceği, teknolojik gelişmelere ve siber tehditlerin evrimine bağlı olarak şekillenecektir. Makine öğrenmesi ve yapay zekâ gibi gelişmekte olan çığır açıcı yeni teknolojik atılımlar, siber saldırıların önceden tahmin edilip risk analizlerinin yapılması ve önleyici tedbirlerin uygulanabilmesi adına önemli bir unsur olabilirler. Diğer taraftan bu teknolojilerin kötü niyetli amaçlarla kullanılma riski de göz ardı edilmemelidir (Miller & Meshkat, 2022).

2.2.5. Siber Güvenlik Politikalarının Sektörel Etkileri

Siber güvenlik politikalarının sadece bireyler ve devletler üzerinde değil, aynı zamanda farklı sektörler üzerinde de önemli etkileri bulunmaktadır. Özellikle finans, sağlık, enerji ve iletişim gibi kritik altyapıları içeren sektörler, siber saldırılara karşı özellikle hassas konumdadır. Bu sektörlerdeki kuruluşlar, siber güvenlik politikalarını etkili bir şekilde uygulayarak hem kendi varlıklarını hem de müşteri bilgilerini korumak durumundadır (Radu & Smaili, 2022).

2.2.6. Siber Güvenlik Politikalarının Ekonomik Etkileri

Siber güvenlik politikalarının uygulanmaması, ekonomik açıdan da önemli sonuçlar doğurabilir. Özellikle büyük ölçekli siber saldırılar, işletmelerin faaliyetlerini durdurabilir ve milyonlarca dolarlık zarara yol açabilir. Bu nedenle, siber güvenlik politikalarının maliyeti, potansiyel zararları önleme açısından göz ardı edilemeyecek kadar önemlidir (Gordon, 2018).

2.2.7. Siber Güvenlik Politikalarının Yasal Çerçevesi

Siber güvenlik politikalarının yasal çerçevesi, her ülke açısından aynı olmayabilir fakat genellikle farklılıklar olsa da kişisel verilerin korunması ve siber suçların cezalandırılması gibi konuları yasalarla ve diğer ilgili mevzuatlarla normlar oluşturulmuştur. Bu normlar, siber güvenlik politikalarının uygulanmasını desteklemekte ve tehditlere karşı yasal bir dayanak oluşturmaktadır (Sayedi & Sakallı Büyüksaraçoğlu, 2020).

2.2.8. Siber Güvenlik Politikalarının Toplumsal Etkileri

Siber güvenlik politikalarının toplumsal boyuttaki etkileri de göz önünde bulundurulmalıdır. Özellikle dijital güvenlik bilincinin artırılması ve toplumun genel olarak siber tehditlere karşı daha bilinçli olması, siber güvenlik politikalarının başarılı bir şekilde uygulanmasını sağlayabilir. Ayrıca, siber güvenlik politikalarının adil bir şekilde uygulanması da toplumsal adalet açısından önemlidir (Nguyen & Pham, 2020).

2.2.9. Siber Güvenlik Politikalarının Eğitim ve Farkındalık Boyutu

Siber güvenlik politikalarının etkili bir şekilde uygulanabilmesi adına, farkındalık ve eğitim çalışmalarının ciddi önem arz ettiği yadsınamaz. Kullanıcıların, kurumların ve devletlerin siber tehditlere karşı nasıl korunacaklarını bilmesi ve bilinçli bir şekilde hareket etmeleri, siber güvenlik politikalarının başarısını büyük ölçüde etkileyebilir. Bu nedenle, eğitim programları ve farkındalık kampanyaları düzenlenmelidir (Al-Janabi & AlShourbaji, 2015).

Eğitim programları, siber güvenlik konusunda temel bilgilerin yanı sıra güvenli internet kullanımı, şifre yönetimi ve güvenlik önlemleri gibi pratik bilgileri de içermelidir. Özellikle kurumlar, çalışanlarını düzenli olarak eğitmeli ve güvenlik politikalarını gözden geçirmeleri konusunda teşvik etmelidir (Rezgui & Marks, 2008). Ayrıca, siber güvenlik farkındalık kampanyaları, geniş kitlelere siber tehditlerin farkındalığını artırabilir ve güvenlik bilincinin toplum genelinde yayılmasına yardımcı olabilir (Al-Janabi & AlShourbaji, 2015). Bu eğitim ve farkındalık çalışmaları, siber güvenlik alanındaki politikaların etkin şekilde hayata geçirilmesinde temel bir hamledir. Ancak, sürekli bir eğitim ve farkındalık programının sürdürülmesi de önemlidir. Teknolojik gelişmeler ve yeni tehditler karşısında güncel bilgilere sahip olmak, siber güvenlik açısından kritik öneme sahiptir (Saeed, 2023).

Siber uzayın giderek yaygınlaşmasıyla birlikte, siber tehditlerin de artması kaçınılmazdır. Söz konusu tehditler karşısında etkin bir mücadelede bulunabilmek ve korunabilmek için siber güvenlik alanında politikaların meydana getirilmesi ve uygulamaya konulması zorunludur. Siber güvenlik politikalarının sadece bireyler ve devletler üzerinde değil, aynı zamanda farklı

sektörler ve ekonomik yapılara da önemli etkilerinin olduğu yadsınamaz. Özellikle kritik altyapıları içeren sektörlerin, siber güvenlik politikalarıyla uyumlu davranmaları ve kendilerini korumaları ciddi öneme haizdir. Bir diğer husus; eğitim ve farkındalık çalışmalarının da siber güvenlik alanındaki politikaların etkin derecede uygulamaya konmasında kritik bir rol oynamasıdır ve bu aynı zamanda bu çalışmanın ana unsurlarındandır. Kullanıcıların bilinçli olması ve temel güvenlik önlemlerini bilmesi, siber tehditlere karşı en etkili savunma mekanizmalarından biridir. Siber güvenlik politikalarının geliştirilmesi ve sahaya yansımaları, günümüz dijital çağında kaçınılmaz bir gerekliliktir. Bu politikaların etkin derecede uygulamaya konulabilmesi, bireylerin, kurumların ve devletlerin siber tehditlere karşı korunmasını sağlayacak ve dijital dünyada güvenli bir ortamın oluşturulmasına katkıda bulunacaktır.

2.3. SİBER GÜVENLİK EĞİTİMİNE DAİR TEMEL KAVRAMLAR

Siber güvenlik gerektiren siber uzay unsurları, kişisel yaşamlarımızın ve kurumsal olarak da devletlerin her alanına nüfuz etmektedir. Dolayısıyla, siber uzayda yaşam temel becerilerinden başlanmak üzere en önemlisi de siber uzayda hem bireylerin hem de devletlerin korunabilmesi için siber güvenlik eğitiminin tüm eğitim düzeylerine entegre edilmesi yaşamsal bir zorunluluk haline gelmektedir.

Genel olarak eğitim programlarını da kapsayacak şekilde, çeşitli disiplinlerden seçmeli derslerde, disiplinler arası şekilde gerek alt başlıklar olarak gerekse de siber uzayla ilgili çok sayıda ana dalda siber güvenliğe dair bilgiyi eğitim sisteminin müfredatına resmî olarak yer alması günümüzün gereği haline gelmiştir. Kapsayıcı bir bakış açısıyla; hem formal[1] eğitimin içerisinde yani sınıf içinde derslerde hem de informal eğitim boyutunda okul dışı ortamlarda siber güvenlik bilincini ve siber güvenlik bilgi ve becerilerinin hem kazanıldığı hem de uygulanabildiği bir siber güvenlik eğitimi ideal bir siber güvenli toplum – devlet örneğini ifade etmektedir.

[1] Formal eğitimde belirli bir yapılandırma, ortam, müfredat ve kurallar dizisi söz konusundur, informal eğitim ise doğal çevrede ve yapılandırılmadan kendiliğinden gelişir.

Siber güvenlik; düşmanlara karşı kişilerden, bilgilerden ve süreçlerden emin olunmasını sağlamak için bilgisayar temelli teknolojileri içeren bir disiplinde güvenli bilgisayar sistemlerinin oluşturulmasını, çalıştırılmasını, analizini ve testini içermektedir. Dolayısıyla *siber güvenlik eğitimi* hukuk, politika, insan faktörleri, etik ve risk yönetimi gibi alanların hepsini ilgilendiren disiplinler arası bir eğitimi ifade etmektedir (ACM, 2017).

Siber güvenlik eğitimi; farklı seviyelerde teknik olan ve teknik olmayan içeriklerden meydana gelmelidir (Austin, 2020):

- Genel eğitim içeriği tüm öğrencilere siber güvenliğin temellerinin aktarılmasını ifade etmelidir.
- Siyaset bilimi, hukuk, bilgisayar bilimleri gibi alanlarda disipliner ve disiplinler arası siber seçmeli derslerle kişinin eğitimini siber güvenlikle ilgili içeriklerle desteklemek açısından önemli fırsatlar sağlanmalıdır.
- Siber güvenlik mühendisliği veya robotik gibi seçmeli veya ağırlıklı siber güvenlik odaklı siber güvenlik yan dalından az, ancak tek bir kurstan daha fazla uzmanlaşma fırsatı sağlanmalıdır.
- Aynı anda teknik olan ve teknik olmayan siber güvenlik alanlarında uzmanlaşılmalıdır.
- Teknik veya teknik olmayan siber güvenlik bölümlerinden mezunlar siber uzayda güvenliği sağlamada başarılı olmaya hazırlanmalıdır.

Austin'e göre, siber güvenlik eğitimi, teknik ve teknik olmayan içeriklerin bir araya geldiği çok disiplinli bir alan olarak tanımlanmakta ve bu alandaki eğitim, sadece teknik becerilerin değil, aynı zamanda politika, hukuk ve etik gibi teknik olmayan konuların da öğretilmesini gerektirmektedir (Austin, 2020).

Şekil 1 *Bütünsel Siber Eğitimin Müfredat Öğeleri (Austin, 2020)*

United States Military Academy (USMA), Birleşik Devletler Ordu Akademisi bilişim disiplininde, bilişim disiplini dışında ya da disiplinler arası olmak üzere seçmeli dersler imkanı tanımaktadır. Bu seçmeli derslerden en popüler olanlar (USMA, 2016).

- *Bilgisayar Bilimleri kursu CS483*
- *Dijital Adli Tıp*
- *Bilgisayar Bilimleri Özel Konular kursu CS485 Etik Hacking*
- *Siber Mühendislik kursu CY450 Siber Güvenlik Mühendisliği*
- *Siber Bilim kursu CY383*
- *Güvenli Arayüz Tasarımı*
- *Siber Bilim kursu CY460 Siber Politika, Strateji ve Operasyonlar*
- *Elektrik Mühendisliği Özel Konular kursu EE485*
- *Donanım Hacking*
- *Mühendislik Psikolojisi kursu PL475*
- *İnsan-bilgisayar Etkileşimi*
- *Tarih kursu XH341*
- *Siber İstihbarat Tarihi*
- *Bilgi Teknolojisi Özel Konular Kursu IT485*

- *Zekâ Analizinin İlkeleri*
- *Hukuk kursu LW462*
- *Siber Hukuk*
- *Matematik kursu MA464*
- *Kriptoloji ile Uygulamalı Cebir*
- *Felsefe kursu PY326*
- *Siber Etik.*

Avrupa Birliği (AB) açısından duruma bakıldığında AB bu tehditlere karşı etkin şekilde mücadele etmek için iyi bilgilendirilmiş ve siber okuryazar bir nüfusa ihtiyaç olduğunu kabul etmektedir.

Avrupa Birliği kurumsal şemsiyesi altında kurulu olan European Union Agency for Cybersecurity (ENISA) siber güvenlik eğitimini desteklemek için önemli bir rol oynamaktadır. ENISA, üye devletlerdeki siber güvenlik eğitimini koordine eder, en iyi uygulamaları paylaşır ve farkındalığı artırmak için çeşitli programlar yürütür. Ajans, siber güvenlik alanında uzmanlar arasında iş birliği sağlar ve eğitim materyalleri geliştirir (ENISA, 2022a).

Avrupa Birliği üye ülkelerinde ulusal düzeydeki girişimler incelendiğinde Safer Internet Centers (SIC) dilimize Daha Güvenli İnternet Merkezleri olarak çevirebileceğimiz merkezler, Avrupa Komisyonu tarafından finanse edilen ve farklı yaş grupları arasında siber güvenlik farkındalığını artırmayı amaçlayan önemli bir girişimdir. Bu merkezler, ebeveynler, öğretmenler ve gençler için kaynaklar sunar. Ayrıca siber zorbalık, veri gizliliği ve dijital güvenlik konularında eğitimler düzenler. Safer Internet Centers, üye devletler arasında iş birliği platformları olarak da hizmet verir (ENISA, 2022b).

AB üyesi devletlerin farklı eğitim sistemleri olduğundan, siber güvenlik eğitimini tüm müfredatlara entegre etmek zordur. Ancak bu çeşitlilik, farklı yaklaşımları ve en iyi uygulamaları paylaşma fırsatı sunar. Siber güvenlik eğitimini resmî müfredatlara entegre etmek için eğitim kurumları, endüstri ve hükümet arasında iş birliği gereklidir. Bu, siber güvenlik bilincini artırmak için önemlidir. Siber güvenlik eğitimi, teknik, hukuki ve davranışsal yönleri içeren disiplinler arası bir yaklaşımı kapsamalıdır. Teknik becerilerin yanı sıra hukuki ve etik konular da vurgulanmalıdır. Siber güvenlik eğitimi, hayat boyunca

güncellenmesi gereken bir eğitim süreci olarak görülmelidir. Bireyler teknoloji ve tehditler hakkında güncel ve uyanık kalabilmek için sürekli öğrenmeye teşvik edilmelidirler. AB, siber güvenlik eğitimine olan taahhüdünü sürdürmektedir. İyi tasarlanmış politika çerçeveleri, iş birliği ve eğitim programları ile siber güvenlik farkındalığını artırmayı amaçlamaktadır. Böylelikle siber tehditler karşısında çok daha mukavemetli bir toplum inşa edilebilir (European Commission, 2013, p. 8).

3. SİBER GÜVENLİK POLİTİKALARINDA EĞİTİM

Günümüz dünyasında, siber tehditlerin yaygın ve giderek daha karmaşık hale gelmekte olduğu bir ortamda, siber güvenlik politikaları konusundaki eğitimin önemi yadsınamaz. Etkili siber güvenlik eğitimi, dayanıklı bir dijital ortam oluşturmanın temel taşını oluşturur ve bireyler ile kuruluşları hassas bilgileri ve altyapıyı korumak adına gerekli olan becerilerle ve bilgilerle donatır. Bu bölüm, siber güvenlik politikalarında eğitimin kritik rolünü incelemekte ve siber güvenlik farkındalığını ve yeteneklerini artırmaya yönelik büyük ülkelerin ve uluslararası derneklerin eğitim politikalarını detaylandırmaktadır (ITU, 2021).

3.1. SİBER GÜVENLİK POLİTİKALARINDA SİBER GÜVENLİK EĞİTİMİNİN ÖNEMİ

Siber güvenlik eğitimi, siber tehditlerle ilişkili risklerin azaltılmasında önemli bir rol oynar. Eğitim, güvenlik farkındalığı kültürü oluşturur, en iyi uygulamaları teşvik eder ve her seviyedeki bireylerin dijital varlıkları korumadaki rollerini ve sorumluluklarını anlamalarını sağlar. Çeşitli çalışmalar, insan hatasının siber güvenlik ihlallerinde kayda değer bir unsur olduğuna işaret etmektedir ve eğitim bu zayıflığın giderilmesinde esastır (Rezgui & Marks, 2008).

Siber güvenlik alanındaki eğitim, şifre yönetimi, güvenli internet kullanımı, veri koruma ve olay müdahalesi gibi geniş bir yelpazeyi kapsar. Etkili eğitim programları, okul çocuklarından kurumsal çalışanlara ve devlet görevlilerine kadar farklı hedef kitlelerin ihtiyaçlarını karşılayacak şekilde tasarlanmıştır. Siber güvenliğin eğitim müfredatına entegre edilmesiyle, toplumlar dijital çağın getirdiği zorluklarla başa çıkmaya daha hazırlıklı bir nesil yetiştirebilir (Al-Janabi & AlShourbaji, 2015).

Siber güvenlik eğitiminin önemli unsurlarından biri de eleştirel düşünme becerilerinin geliştirilmesidir. Siber tehditler evrildikçe, onlarla mücadele stratejileri de evrilmelidir. Problem çözme ve analitik becerilere vurgu yapan eğitim programları, bireylerin potansiyel tehditleri öngörmelerini ve etkin derecede karşılık vermelerini sağlar. Ayrıca, sürekli öğrenme ve profesyonel

gelişim, siber güvenlik ortamının sürekli değişen yapısında etkili kalmak için çok önemlidir. Profesyonellerin, rollerinde etkili kalabilmek için en son tehditler ve teknolojiler konusunda güncel kalmaları gerekir (Siponen & Vance, 2010).

Güvenlik bilincine sahip bir kültür oluşturma konusunda eğitimin rolü yadsınamaz. Bireyler potansiyel tehditlerin farkında olduklarında ve güvenlik protokollerine uymanın önemini anladıklarında, bir kuruluşun veya topluluğun genel güvenlik duruşu önemli ölçüde artar. Bu kültürel değişim siber güvenlik stratejisinin sürdürülebilir başarısı için gereklidir (NIST, 2017).

3.2. BAŞAT DEVLETLERDE SİBER GÜVENLİK EĞİTİMİ POLİTİKALARI

3.2.1. Amerika Birleşik Devletleri

ABD'de siber güvenliğe "Bilgi Güvenliği" olarak yaklaşılmaktadır. Siber saldırıları ve olayları, federal hükümetin, eyalet ve yerel yönetimlerin, özel sektörün ve kamunun koordineli ve odaklanmış çabalarıyla aşılabilecek stratejik zorluklar olarak ele almaktadır (Karataş, 2020).

ABD siber güvenlik eğitimini çeşitli eğitim seviyelerine entegre eden kapsamlı bir yaklaşım benimsemiştir. NIST tarafından yönetilen Ulusal Siber Güvenlik Eğitimi İnisiyatifi (NICE), ülke genelinde siber güvenlik farkındalığını ve becerilerini artırmaya yönelik koordineli bir çabanın başlıca örneğidir. NICE, eğitim programları, sertifikalar ve iş gücü eğitimini geliştirmeye odaklanır ve siber güvenlik alanındaki değişen ihtiyaçlara cevap verir (NICE, 2017).

Department of Homeland Security (DHS- Amerika Birleşik Devletleri İç Güvenlik Bakanlığı) de Cybersecurity and Infrastructure Security Agency (CISA- Siber Güvenlik ve Altyapı Güvenliği Ajansı) gibi girişimler siber güvenlik eğitiminin teşvik edilmesinde önemli bir rol oynar. CISA, eğitimciler, öğrenciler ve profesyoneller için kaynaklar ve eğitim programları sunar. Ayrıca, CyberCorps®: Hizmet için Burs Programı, kamu sektöründe çalışmayı taahhüt eden öğrencilere siber güvenlik dereceleri için burs sağlar ve böylece siber güvenlik iş gücünü güçlendirir (USCYBERCOM, 2021).

ABD Siber Komutanlığı da askeri eğitimde siber güvenlik eğitimini entegre etmek için çeşitli girişimler başlatmıştır. Bu yaklaşım, askeri personelin siber savunma tekniklerinde iyi eğitim almasını sağlayarak ulusal güvenliğe katkıda bulunur. Askeri akademiler ve eğitim programlarında siber güvenlik eğitimine yapılan vurgu, siber güvenliğin ulusal savunmadaki stratejik önemini vurgular (DHS, 2020).

Kurumsal sektörde, Google ve Microsoft gibi kuruluşlar, çalışanları için kapsamlı siber güvenlik eğitim programları geliştirmiştir. Bu programlar genellikle siber saldırı simülasyonlarını içerir ve çalışanların potansiyel tehditleri tanımasını ve kontrol altında bir ortamda yanıt vermesini sağlar. Bu tür pratik eğitim, bireylerin gerçek dünyadaki siber güvenlik zorluklarıyla başa çıkmaya hazırlıklı olmaları için gereklidir (McAfee, 2020).

3.2.2. İngiltere

İngiltere'de siber güvenlik konusundaki araştırma özetinde, siber tehditlerin çok çeşitli aktörlerden geldiği belirtilmektedir. Bu aktörler arasında devlet ve devlet destekli gruplar, mali çıkar amaçlı organize suç örgütleri ve politik amaçları olan 'hacktivist' gruplar yer almaktadır. Devlet destekli grupların, özellikle Rusya, Çin, İran ve Kuzey Kore'nin, İngiltere'nin çıkarlarına yönelik siber tehditleri oluşturduğu vurgulanmaktadır. Bu tehditlerin, hükümet ve siyasi aktörler, kritik ulusal altyapı ve sivil toplum kuruluşları gibi hedeflere yönelik olduğu belirtilmektedir. Ayrıca, organize suç gruplarının, genellikle mali kazanç peşinde koşan, Doğu Avrupa menşeli Rusça konuşan gruplar olduğu ve bu grupların karmaşık yapılar ve yönetim sistemlerine sahip oldukları ifade edilmektedir (Clark, 2024, s. 7-8).

İngiltere'nin siber güvenlik düzenleyici çerçevesi, birden fazla birincil ve ikincil mevzuattan kaynaklanmaktadır. Farklı mevzuatlar, BT sistemlerinin, internete bağlı ürünlerin ve kişisel verilerin siber güvenliğini kapsamaktadır. Siber güvenlik mevzuatındaki yasal yükümlülükler, siber güvenlik ihlallerinin toplum, ekonomi veya bireysel haklar üzerinde önemli etkileri olabilecek sektörler ve kuruluşlar için geçerlidir. Bu sektörler arasında telekomünikasyon ve ulaşım gibi temel hizmet sağlayıcıları ile dijital hizmet sağlayıcıları bulunmaktadır. Hükümet, kritik ulusal altyapı sağlayıcılarına düzenli ve sürekli

erişim sağlayan BT hizmetleri sunan sunucu sağlayıcıların bu düzenlemelere tabi olmasını hedeflemektedir. Ayrıca, etik hacker'lar için yasal savunma sağlanmasının yasaklanması gibi reform önerileri de bulunmaktadır (Clark, 2024, s. 43-52).

Siber saldırıların gerçek ölçeğini ve maliyetini anlamak zordur, çünkü mevcut veriler büyük ölçüde kendiliğinden raporlamaya dayanmaktadır. Hükümetin Siber İhlal Anketi ve Siber Güvenlik Uzunlamasına Anketi, İngiliz işletmelerinin siber güvenlik deneyimlerini yıllık olarak raporlamaktadır. Daha büyük organizasyonlar, olayları tanımlama kapasitesine daha fazla sahip oldukları için siber saldırı yaşama olasılıkları daha yüksektir. 2024 yılında yapılan anket, işletmelerin yaklaşık yarısının ve hayır kurumlarının üçte birinin son 12 ay içinde bir siber saldırı yaşadığını bildirmiştir. Büyük ölçekli veri ihlalleri, örneğin, 102.000 kayıtlık ihlal, organizasyonlara oldukça fazla maliyeti olmaktadır. Bu bağlamda, İngiltere'deki siber suçların yıllık ekonomik maliyetinin 21 milyar sterlin olduğu tahmin edilmektedir (Clark, 2024, s. 17-19).

Siber güvenlik politikası, İngiltere'de önem verilmiş bir konu olup, birçok ilgili politika alanı gibi ulusal güvenlik, ürün güvenliği ve tüketici koruması da bu kapsamda ele alınmaktadır. 2022 Ulusal Siber Güvenlik Stratejisi İngiltere'nin siber güvenlik politikasını tanımlamakta ve hükümetin özel sektör kuruluşları ve siber güvenlik profesyonelleriyle ortak çalışarak siber güvenliği iyileştirme yaklaşımını benimsediğini ifade etmektedir. Strateji, siber güvenlik yükünü bireysel vatandaşlardan, siber riskleri yönetme konusunda en iyi konumda olan kuruluşlara kaydırmayı amaçlamaktadır. Bu bağlamda hükümet, Ulusal Siber Güvenlik Merkezi'nin siber güvenlik rehberliğinin benimsenmesini ve siber güvenlik önlemlerine yatırım yapılmasını teşvik etmekte, yetenekli siber profesyonellerin sayısını artırmakta ve yasal siber güvenlik sorumluluklarını güçlendirmeyi hedeflemektedir (Clark, 2024, s. 25-28).

Siber güvenlik becerilerinin geliştirilmesi, hükümetin siber güvenlik stratejisinin merkezinde yer almaktadır. Stratejinin vizyonu ve hedefi, gerekli siber güvenlik becerileri ve bilgilerini geliştirmenin yanı sıra, tüm hükümet genelinde bir siber güvenlik kültürü oluşturmayı gerektirmektedir. (Government Cyber Security Strategy, 2022-2030, s. 58).

Hükümet, siber güvenlik yeteneklerinin gereksinimlerini kapsamlı bir şekilde anlayarak bu kapsamda siber güvenlik kariyer yollarını teşvik etmeyi taahhüt etmektedir. Bu süreç, sürdürülebilir bir hükümet siber güvenlik profesyoneli için kariyer imkânı sağlayarak mevcut yetişmiş insan kaynaklarının elde tutulmasının benimsenmesini içermektedir (Government Cyber Security Strategy, 2022-2030, s. 60-62).

Temelde, bu strateji, insanların öğrenmeye, sorgulamaya dayanan bir siber güvenlik kültürü oluşturmanın önemini vurgulayarak siber güvenlik kültürü oluşturmayı hedefler (Government Cyber Security Strategy, 2022-2030, s. 63).

Bu temeller üzerine inşa edilecek strateji, tüm bireylerin kurumsal siber güvenlik risklerine proaktif bir şekilde katılmasını teşvik eden pozitif bir siber güvenlik kültürü oluşturulacaktır (Government Cyber Security Strategy, 2022-2030, s. 63).

3.2.3. Almanya

Almanya'nın siber güvenlik eğitimi ve politikaları, ülkedeki dijital dönüşümü güvence altına almak amacıyla geliştirilmiş ve geniş kapsamlı stratejiler üzerine inşa edilmiştir. Bu stratejiler, federal hükümetin, özel sektörün, araştırma topluluklarının ve sivil toplumun iş birliğini gerektiren çok disiplinli bir yaklaşımı benimsemektedir.

3.2.3.1.Siber Güvenlik Stratejisi 2021:

Almanya'nın 2021 Siber Güvenlik Stratejisi, siber güvenliğin tüm paydaşlar arasında ortak bir sorumluluk olarak ele alınmasını sağlamayı hedeflemektedir. Strateji, dijital egemenliği güçlendirme, güvenli dijital dönüşümü sağlama ve belirlenebilir, şeffaf hedefler koyma gibi dört ana ilkeye dayanmaktadır. Ayrıca, hükümetin, özel sektörün ve sivil toplumun etkin bir şekilde iş birliği yapması gerektiğini vurgulamaktadır. Bu strateji, 2011 ve 2016 yıllarında yayımlanan önceki stratejilere dayanmakta ve onların üzerine inşa edilmektedir (Federal Ministry of the Interior, 2021).

3.2.3.2.Almanya'nın Siber Güvenlik Politikası:

Almanya'nın siber güvenlik politikaları, federal hükümetin etkili bir şekilde koordinasyon yapmasını ve dijital egemenliğin korunmasını sağlamak

amacıyla geliştirilmiştir. 1991 yılında kurulan Federal Bilgi Güvenliği Ofisi (BSI), siber güvenlik alanında merkezi bir otorite olarak görev yapmaktadır. BSI, hem kamu sektörü hem de kritik altyapı operatörleri ile yakın iş birliği içinde çalışarak, bilgi güvenliğini sağlamak için çeşitli önlemler almaktadır (Brzostek, 2022).

3.2.3.3.2023 Almanya IT Güvenlik Durumu Raporu:

2023 yılında yayımlanan Almanya IT Güvenlik Durumu Raporu, ülkenin siber güvenlik politikalarının etkinliğini değerlendirmektedir. Bu rapor, Almanya'nın siber güvenlik eğitimine yönelik ihtiyaçlarını ve bu alandaki mevcut tehditleri analiz etmektedir. Raporda, özellikle pandemi dönemi boyunca artan siber saldırılar ve bu saldırılara karşı alınan önlemler vurgulanmaktadır (BSI, 2023).

3.2.3.4.Eğitim ve Farkındalık Programları:

Almanya'da siber güvenlik eğitimi hem teknik becerilerin hem de genel farkındalığın artırılmasına odaklanmaktadır. 2021 Siber Güvenlik Stratejisi, özellikle dijital okuryazarlığı artırmayı hedefleyen çeşitli programlar sunmaktadır. Bu programlar hem okullarda hem de meslek eğitimlerinde dijital güvenlik konusunda bilgi düzeyini artırmayı amaçlamaktadır. Örneğin, Deutschland sicher im Netz e.V. (DsiN- Ağda Güvenli Almanya Derneği) gibi kuruluşlar, dijital güvenlik konusunda halkı ve küçük işletmeleri desteklemek için çeşitli inisiyatifler sunmaktadır. Ayrıca, federal hükümetin dijital okuryazarlık artırma programları kapsamında, bireylere ve küçük işletmelere yönelik dijital güvenlik konusunda farkındalık yaratmak için özel rehberlik sağlanmaktadır (Taylor-Jackson et al., 2020; Federal Ministry of the Interior, 2021).

3.2.3.5.Araştırma ve Geliştirme Programları:

Almanya, siber güvenlik alanında dünya çapında tanınan araştırma merkezlerine ev sahipliği yapmaktadır. ATHENE (Darmstadt), CISPA (Saarbrücken) ve KASTEL (Karlsruhe) gibi ulusal mükemmeliyet merkezleri, bu alanda ileri düzey araştırmalar yapmaktadır. Federal Eğitim ve Araştırma Bakanlığı, bu merkezlerde kurulan iş kuluçka merkezleri aracılığıyla yeni girişimlerin kurulmasını desteklemektedir. Ayrıca, "Digital. Sicher. Souverän."

isimli IT güvenliği araştırma programı, Almanya'nın IT güvenliği araştırmalarını kararlılıkla ileriye taşımayı hedeflemektedir (Brzostek, 2022).

3.2.3.6.Siber Güvenlik Eğitimine Yönelik Devlet Desteği:

Almanya'da siber güvenlik eğitimi, devlet tarafından da aktif bir şekilde desteklenmektedir. Örneğin, Universität der Bundeswehr München bünyesindeki CODE Research Institute hem askeri personel hem de federal hükümet çalışanları için temel ve ileri düzey siber güvenlik eğitimi sağlamaktadır. Bu eğitimler, dijital dönüşümün güvenli bir şekilde gerçekleştirilmesi için kritik bir rol oynamaktadır (Taylor-Jackson et al., 2020).

3.2.4. Çin

Çin'in siber güvenlik eğitimine yaklaşımı, ulusal güvenlik ve devlet kontrolüne güçlü bir vurgu yapmaktadır. Çin hükümeti, ilk okullardan üniversitelere kadar ulusal eğitim sistemine siber güvenlik eğitimini entegre etmiştir. 2017 yılında yürürlüğe giren Çin Halk Cumhuriyeti Siber Güvenlik Yasası, eğitim kurumlarının müfredatlarına siber güvenlik farkındalığını dahil etmelerini zorunlu kılmaktadır (Dakota, 2021).

Çin hükümeti ayrıca siber güvenlik araştırma ve geliştirmelerine büyük yatırımlar yaparak yenilikçiliği teşvik eden ve ülkenin siber savunma yeteneklerini artıran girişimleri desteklemektedir. Üniversiteler ve araştırma kurumları, endüstri ve kamu kuruluşlarıyla iş birliği içerisinde ileri teknolojiler ve eğitim programları geliştirmeye teşvik edilmektedir (Dakota, 2021).

Ayrıca, Çin, Wuhan'daki Ulusal Siber Güvenlik Yetenek ve İnovasyon Üssü gibi birçok siber güvenlik eğitim merkezi ve akademisi kurmuştur. Bu kurumlar, ülkenin siber güvenlik zorluklarına yanıt verebilecek ve küresel siber güvenlik çabalarına katkıda bulunabilecek yetenekli bir iş gücü geliştirmeye odaklanmaktadır (Dakota, 2021).

Bu kapsamda Çin'de konunun sahada pekiştirilmesini sağlayan eğitim çalışmaları da yapılmaktadır. Örneğin, Cheung ve Cohen (2011), siber güvenlik eğitiminde yenilikçi yöntemler kullanmanın öğrenci öğrenimini önemli ölçüde artırabileceğini vurgulamaktadır. Yazarlar, Zorluk Tabanlı Öğrenme (CBL) metodolojisini uygulayarak, öğrencilerin akranlarıyla iş birliği

yapmalarını, sorular sormalarını, konuyu daha derinlemesine anlamalarını ve gerçek dünya zorluklarını çözme konusunda harekete geçmelerini teşvik etmişlerdir. Çalışmada, öğrencilerin bilgi güvenliği konusundaki ilgilerini yansıtan temel sorular belirledikleri, siber saldırılardan gizli bilgileri nasıl koruyacaklarına dair zorluklar formüle ettikleri ve ardından bilgilerini ve ağlarını güvence altına almak için çözümler ürettikleri belirtilmektedir (s. 9-11).

Yazarlar, öğrencilerin siber güvenlik becerilerini geliştirmek için yarışmalara katılmalarının ideal bir ortam sağladığını ifade etmektedirler. Cheung ve Cohen, öğrencilerin Siber Savunma Yarışması gibi yarışmalara katıldıklarını ve bu yarışmalarda, öğrencilerin gerçek dünya senaryolarında siber saldırılara karşı savunma yapma ve saldırı gerçekleştirme becerilerini geliştirdiklerini belirtmişlerdir. Yarışmalar sonrası yapılan değerlendirmelerde, öğrencilerin bilgisayar ve güvenlik becerilerinde, güvenlik öğrenme ilgilerinde ve başkalarına öğretme yeteneklerinde önemli iyileşmeler gözlenmiştir (s. 12-15).

Sonuç olarak, Cheung ve Cohen, CBL metodolojisinin siber güvenlik eğitiminde etkili bir öğrenme yöntemi olduğunu öne sürmektedirler. Bu metodolojinin öğrenci merkezli ve çok disiplinli bir yaklaşım sunduğunu ve öğrenci öğrenimini nasıl geliştirdiğini vurgulamaktadırlar. Öğrencilerin, pratik uygulamalar ve yarışmalar aracılığıyla bilgilerini pekiştirdiklerini ve siber güvenlik konusuna olan ilgilerini artırdıklarını ifade etmektedirler. Bu çalışma, CBL metodolojisinin, öğrencilerin gerçek dünya problemlerini çözme yeteneklerini geliştirirken aynı zamanda motivasyonlarını ve öğrenme isteklerini artırabileceğini göstermektedir (s. 16-17).

3.2.5. Hindistan

Hindistan, hızla büyüyen dijital ekonomisini koruma konusunda siber güvenlik eğitiminin önemini kabul etmiştir. 2013 Ulusal Siber Güvenlik Politikası, siber güvenlik eğitimi ve farkındalığına kapsamlı bir yaklaşım ihtiyacını vurgulamaktadır. Politika, okul ve üniversite müfredatlarına siber güvenlik konularının dahil edilmesini ve profesyoneller için özel eğitim programlarının kurulmasını savunmaktadır (MEITy, 2013).

Hint hükümeti, Bilgi Güvenliği Eğitim ve Farkındalık (ISEA) projesi gibi çeşitli girişimler başlatmıştır. Bu proje, öğrencilere, eğitimcilere ve profesyonellere yönelik eğitim ve sertifikasyon programları sağlayarak ülkenin siber güvenlik yeteneklerini artırmayı amaçlamaktadır (ISEA, 2020).

Ayrıca, NIELIT ülke genelinde siber güvenlik eğitim ve öğretim programlarının geliştirilmesinde ve sunulmasında merkezi bir rol oynamaktadır. NIELIT, akademik kurumlar, devlet kurumları ve endüstri ortaklarıyla iş birliği yaparak programlarının mevcut endüstri standartlarına ve en iyi uygulamalara uygun olmasını sağlamaktadır (NIELIT, 2021).

3.2.6. Avustralya

Avustralya'nın siber güvenlik eğitimine yaklaşımı, siber konusunda bilinçli bir ulus oluşturmayı vurgulayan Avustralya Siber Güvenlik Stratejisi ile yönlendirilir. Strateji, okul çocuklarından yaşlı vatandaşlara kadar toplumun tüm seviyelerinde siber güvenlik eğitimini ve farkındalığını artırmak için önlemleri içermektedir (ACCS, 2019).

Avustralya hükümeti, kapsamlı siber güvenlik eğitim programları geliştirmek için eğitim kurumları, uluslararası kuruluşlarla ve endüstri ortaklarıyla iş birliği yapmaktadır. AustCyber'ın Okullar Siber Güvenlik Zorlukları gibi girişimler, öğrencilere siber güvenlik konusunda kritik beceriler ve bilgi kazandıran etkileşimli öğrenme deneyimleri sunmaktadır (AustCyber, 2021).

Ayrıca, Avustralya'nın yüksek öğretim sektörü, siber güvenlik araştırmalarında ve eğitiminde kritik rol oynamaktadır. Ülke genelindeki üniversiteler, öğrencilere bu hızla gelişen alanda kariyer yapmaları için hazırlayan özel dereceler ve sertifikalar sunmaktadır. Avustralya Siber Güvenlik Merkezi (ACCS) gibi araştırma merkezleri, ileri düzey araştırmalar yürütmekte ve ülkenin siber savunma yeteneklerini artırmak için eğitim sağlamaktadır (International Information System Security Certification Consortium (ISC)², 2020).

3.2.7. Rusya

Rusya, siber güvenlik eğitimine yönelik sağlam bir yaklaşım benimsemiş olup, siber savunma ve bilgi güvenliğine stratejik olarak önem vermektedir. Rus

hükümeti, ilk eğitimden yüksek öğretime ve profesyonel eğitime kadar ulusal eğitim sistemine siber güvenlik eğitimini entegre etmiştir. Rusya Federasyonu Eğitim ve Bilim Bakanlığı, tüm eğitim kurumlarının müfredatlarına siber güvenlik konularını dâhil etmelerini zorunlu kılarak hem pratik becerilere hem de teorik bilgiye vurgu yapmaktadır (OECD, 2015).

Rus üniversiteleri, siber güvenlik eğitiminde önemli bir rol oynamaktadır. Moskova Devlet Teknik Üniversitesi (Bauman Moskova Devlet Teknik Üniversitesi) ve Ulusal Nükleer Araştırma Üniversitesi MEPhI (Moskova Mühendislik Fizik Enstitüsü) gibi kurumlar, bilgi güvenliği ve siber savunma konularında uzmanlaşmış programlar sunmaktadır. Bu programlar, öğrencilerin kriptografi, ağ güvenliği ve siber istihbarat konularında ileri beceriler kazanmasını amaçlamaktadır (International Organization for Standardization (ISOC), 2020).

Rus hükümeti ayrıca, Federal Güvenlik Servisi (FSB) ve Savunma Bakanlığı gibi çeşitli siber güvenlik eğitim merkezleri ve akademilerini işletmektedir. Bu kurumlar, askeri ve istihbarat personeline siber operasyonlar ve bilgi savaşı konularında ileri eğitim sağlar. Bu kurumlar, siber taktikler, teknikler ve prosedürler konusunda yüksek düzeyde uzmanlık geliştirmeye odaklanmaktadır (Saeed, 2023).

Ek olarak, Rusya, genel kamuoyunda siber güvenlik farkındalığını artırmak için çeşitli girişimler uygulamaktadır. Güvenli İnternet Ligi gibi hükümet dışı örgütler, çocuklar ve yetişkinler arasında siber hijyen ve farkındalığı artırmayı amaçlayan kampanyalar ve eğitim programları düzenlemek için hükümetle iş birliği yapmaktadır. Bu programlar, atölye çalışmaları, online kurslar ve kamu farkındalık kampanyalarını içermektedir (The National Cyber Security Centre (NCSC), 2020).

Rusya'nın siber güvenlik eğitimine yönelik yaklaşımı, uluslararası iş birlikleri tarafından da desteklenmektedir. Ülke, uluslararası forumlara aktif olarak katılmakta ve siber güvenlik eğitim ve öğretiminde en iyi uygulamaları geliştirmek ve uygulamak için diğer kuruluşlarla ve ülkelerle iş birliği yapmaktadır. Bu uluslararası angajman, Rusya'nın siber güvenlik konusundaki

küresel trendleri ve gelişmeleri takip etmesine yardımcı olmaktadır (Cybersecurity & Infrastructure Security Agency (CISA), 2021).

3.3. ULUSLARARASI KURULUŞLAR

Uluslararası dernekler, siber güvenlik eğitimini teşvik etmek ve küresel iş birliğini desteklemek konusunda hayati bir rol oynamaktadır.

AB, siber güvenlik eğitiminde çok yönlü bir yaklaşım benimsemiş, sınır ötesi iş birliği ve eğitim standartlarının uyumlaştırılmasının önemini vurgulamıştır. ENISA, bu çabaların ön saflarında yer almakta, üye ülkelerde siber güvenlik farkındalığını ve yeteneklerini artırmak için yönergeler, kaynaklar ve eğitim programları sunmaktadır (European Commission, 2020).

ENISA'nın girişimleri arasında Avrupa Siber Güvenlik Ayı (ECSM- European Cyber Security Month) yer alır ve bu etkinlikler, kampanyalar ve eğitim faaliyetleri aracılığıyla siber güvenlik tehditlerine dair farkındalık oluşturmayı ve en iyi uygulamaları teşvik etmeyi amaçlar. Ajans ayrıca, bir sonraki profesyonel neslin Avrupa'nın dijital altyapısını koruma konusunda gereken yeteneklere haiz olmasını sağlamak adına eğitim kurumlarıyla iş birliği yaparak siber güvenlik müfredatları ve eğitim programları geliştirmektedir (ENISA, 2021).

AB ayrıca Dijital Eğitim Eylem Planı'nı da hayata geçirmiştir ve bu plan, eğitimde teknoloji kullanımını destekleme ve vatandaşlar arasında dijital becerileri geliştirme önlemlerini içermektedir. Bu plan, dijital okuryazarlığın güvenli bir dijital ortamı sağlama konusundaki kritik rolünü kabul ederek siber güvenlik eğitimi ve eğitimini geliştirme eylemlerini içermektedir (Cartwright, Hernandez Castro, & Cartwright, 2019)

Uluslararası Telekomünikasyon Birliği (ITU), Uluslararası Bilgi Sistemleri Güvenliği Sertifikasyon Konsorsiyumu (ISC)², NATO, OECD ve İnternet Topluluğu (ISOC) gibi organizasyonlar, dünya çapında tanınan çerçeveler ve sertifikalar sunarak siber güvenlik eğitimi ve öğretimini standartlaştırmaya yardımcı olmaktadır (ENISA, 2020).

Birleşmiş Milletler'in uzmanlaşmış bir ajansı olan ITU, Küresel Siber Güvenlik Gündemi (GCA) ve Çocuk Çevrimiçi Koruma (COP) programı gibi

girişimlerle siber güvenlik farkındalığını ve yeteneklerini artırmaya çalışmaktadır. Bu girişimler, en iyi uygulamaları teşvik ederek ve bilgi paylaşımını kolaylaştırarak siber tehditlere karşı küresel topluluğun yanıt verme yeteneğini artırmayı amaçlamaktadır (ITU, 2021).

Uluslararası Bilgi Sistemleri Güvenliği Sertifikasyon Konsorsiyumu (ISC)², siber güvenlik alanında bireylerin uzmanlıklarını doğrulayan ve endüstride yüksek saygınlığa sahip olan Certified Information Systems Security Professional (CISSP- Sertifikalı Bilgi Sistemleri Güvenliği Uzmanı) gibi küresel olarak olarak tanınan sertifikalar sunmaktadır. Bu sertifikalar, profesyonel yeterliliğin bir ölçütü olarak hizmet etmektedir (Internet Society (ISOC), 2020).

NATO da siber güvenlik eğitimini teşvik etme ve uluslararası iş birliğini destekleme konusunda önemli bir rol oynamaktadır. Estonya'nın Tallinn kentindeki NATO İş Birliği Siber Savunma Mükemmeliyet Merkezi (CCDCOE), ileri düzey eğitimler sağlamakta, NATO'nun ana siber savunma eğitim alanı olarak hizmet vermekte ve NATO üye ülkelerinin ve ortaklarının siber savunma yeteneklerini artırmaya yönelik araştırmalar yapmaktadır. CCDCOE, yıllık olarak düzenlenen Locked Shields tatbikatını organize ederek katılımcı ülkelerin hazırlık ve yanıt verme yeteneklerini geliştirmeyi hedeflemektedir (International Association of Privacy Professionals (IAPP), 2021).

NATO'nun siber güvenlik eğitimi ve eğitim politikaları, üye devletlerin ve ortakların siber savunma yeteneklerini artırmayı amaçlayan kapsamlı ve çok yönlü bir strateji barındırmaktadır. Bu kapsamda kuruluşun siber savunma politikası, NATO ittifakının kendi ağlarının korunması ve üye devletlerin gerektiğinde yardım alabilmesi üzerine odaklanmaktadır. 2014 yılında onaylanan NATO'nun üçüncü gelişmiş Siber Savunma Politikası, siber savunmanın ittifakın kolektif savunma görevinin bir parçası olduğunu açıkça belirtmekle birlikte NATO üyesi ülkelerin kollektif savunma hükmünün (Madde 5) siber saldırılar durumunda da uygulayabileceğini onaylamaktadır (Pernik, 2014).

NCIA 2019 yılında kurulmuş olup, NATO personeline yönelik kapsamlı siber güvenlik ve savunma eğitimleri sunmaktadır. Akademi, NATO'nun teknolojik üstünlüğünü ve operasyonel etkinliğini koruma misyonunu desteklemektedir. NCIA NATO'nun siber savunma yeteneklerini uygulamak, işletmek ve eğitim programları sunmaktan sorumludur (Pernik, 2014). Verilen eğitimler arasında statik ve dağıtılmış NATO iletişim ve bilgi sistemleri, Hava Komuta ve Kontrol konuları bulunur. Programlar, Portekiz'deki ana kampüste ve diğer NATO bölgelerinde uygulanmaktadır. NCIA sürekli olarak yeni öğrenme çözümleri tasarlayıp geliştirerek NATO personelinin mesleki gelişimini teşvik etmektedir (NCIA, n.d.).

Ayrıca NATO ve AB, siber güvenlik konusunda da iş birliği yapmaktadır. Her iki çok uluslu örgüt, siber güvenliğin stratejik bir güvenlik önceliği olduğunu kabul etmekle birlikte iş birliği, farkındalık artırma, ortak eğitimler ve kapasite geliştirme gibi alanlara odaklanmaktadır (Kovács, 2018).

OECD, üye ülkeler arasında siber güvenlik farkındalığını ve eğitimini teşvik eden yönergeler ve tavsiyeler geliştirmiştir. OECD'nin ilkeleri, siber güvenlik eğitimine yönelik koordineli bir yaklaşımın önemini vurgulamakta ve hükümet, endüstri ve akademiyi içine alan bir iş birliğini öne çıkarmaktadır (UNODC, 2021).

Uluslararası Standartlar Organizasyonu (ISO) da bilgi güvenliği yönetiminde en iyi uygulamalar için bir çerçeve sunan standartlar ve yönergeler geliştirerek siber güvenlik eğitimine katkıda bulunmaktadır. Örneğin, ISO/IEC 27001, bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesi için gereksinimleri belirler (Internet Society (ISOC), 2020).

Küresel bir kâr amacı gütmeyen organizasyon olan İnternet Topluluğu (ISOC-Internet Society), siber güvenlik eğitimi ve güvenli bir internet ortamını teşvik etmede kritik bir rol oynamaktadır. ISOC'un girişimleri, Online Güvenilirlik İttifakı (OTA- Online Trust Alliance) ve İnternet Yönetişim Forumu (IGF-Internet Governance Forum) gibi girişimler, küresel çapta siber güvenlik farkındalığını artırmayı ve en iyi uygulamaların benimsenmesini teşvik etmeyi hedeflemektedir (National Cyber Security Centre [NCSC], 2021). Ayrıca,

Uluslararası Gizlilik Profesyonelleri Birliği (IAPP- International Association of Privacy Professionals), gizlilik ve veri koruma konularında eğitim ve profesyonel sertifikasyonlar sunarak bu alanda öncü bir rol oynamaktadır. IAPP, Gizlilik Bilgi Profesyoneli Sertifikası (CIPP- Certified Information Privacy Professional) ve Gizlilik Yönetimi Sertifikası (CIPM- Certified Information Privacy Manager) gibi sertifikalar sunarak bireylerin gizlilik ve veri koruma konularındaki bilgi ve becerilerini doğrular (National Institute of Standards and Technology [NIST], 2020).

Olay Yanıt ve Güvenlik Takımları Forumu (FIRST) de küresel siber güvenliği geliştirmeyi amaçlayan önemli bir uluslararası organizasyondur. FIRST, üyeleri arasında iş birliğini ve bilgi paylaşımını teşvik ederek küresel siber güvenliği artırmayı amaçlamaktadır. FIRST'in girişimleri, dünya çapındaki olay yanıt ekiplerinin yeteneklerini artırmak için eğitim ve kaynaklar sağlamayı içerir (FIRST, 2021).

Küresel Siber Uzmanlık Forumu (GFCE), siber kapasite geliştirme ve siber güvenlik becerilerinin geliştirilmesini teşvik eden uluslararası bir platformdur. GFCE, hükümetler, uluslararası kuruluşlar ve özel sektör arasında iş birliğini kolaylaştırarak siber güvenlik eğitimini, eğitimini ve en iyi uygulamaların paylaşılmasını teşvik eder (Global Forum on Cyber Expertise (GFCE), 2021).

Son olarak, APEC, Asya-Pasifik bölgesinde siber güvenliği artırmayı amaçlayan APEC Siber Güvenlik Stratejisi'ni uygulamaya koymuştur. APEC'in girişimleri, üye ekonomilerin siber güvenlik becerilerini artırmak için iş birliği gayretlerini, eğitim programlarını ve atölye çalışmalarını içerir (Asia-Pacific Economic Cooperation (APEC), 2021).

Sonuç olarak, siber güvenlik eğitimi, etkili siber güvenlik politikalarının temel bir bileşenidir. Bireyleri ve kuruluşları gerekli bilgi ve becerilerle donatarak, eğitim riskleri azaltmaya, güvenlik farkındalığı kültürü oluşturmaya ve dijital altyapıların dayanıklılığını sağlamaya yardımcı olur. Hem ülkeler hem de uluslararası dernekler, siber güvenlik eğitimini politikalarına ve stratejilerine entegre etmenin önemini kabul etmekte, bu da küresel çapta siber güvenlik yeteneklerini artırmaya ve dijital ekosistemi korumaya yönelik bir taahhüdü yansıtmaktadır.

Siber güvenlik, modern dijital çağda önemli bir konu haline gelmiştir. Kurumlar ve bireyler, siber tehditlerle başa çıkmak için çeşitli önlemler alırken, siber güvenlik eğitimi de büyük bir rol oynamaktadır. Ancak, teknolojik önlemler kadar, insan unsurunun da bu eğitimlerdeki önemi göz ardı edilmemelidir.

3.4. SİBER GÜVENLİK EĞİTİMİ POLİTİKALARINDA İNSAN UNSURU

Siber güvenlik, günümüz dijital dünyasında kritik bir öneme sahiptir. Kurumlar ve bireyler, siber tehditlerle başa çıkmak için çeşitli teknolojik çözümler geliştirirken, insan faktörünün de bu süreçteki rolü giderek daha fazla vurgulanmaktadır. İnsan unsuru, siber güvenlik eğitim politikalarının başarısında kilit bir bileşen olarak karşımıza çıkmaktadır. Eğitim programları, bireylerin siber tehditlere karşı farkındalıklarını artırmayı ve güvenli davranış alışkanlıkları kazandırmayı amaçlamaktadır. Bu bağlamda, siber güvenlik eğitimlerinde insan unsurunun önemi hem bireysel hem de kurumsal düzeyde güvenlik kültürünün oluşturulmasında belirleyici bir rol oynamaktadır. Siber tehditlerin sürekli evrildiği bir ortamda, insan faktörüne odaklanan eğitim stratejileri, sadece teknolojik önlemlerle sınırlı kalmayan kapsamlı bir güvenlik yaklaşımını gerektirmektedir.

3.4.1. Eğitim ve Farkındalık

Siber güvenlik eğitiminde insan unsurunun önemi, farkındalık yaratma ve bilgi artırma açısından büyük rol oynamaktadır. "Siber güvenlikte insan faktörü, organizasyonların güvenlik politikalarının başarısında kritik bir bileşendir" (STM ThinkTech, 2020). Bu nedenle, çalışanların siber tehditlere karşı bilinçlendirilmesi ve doğru davranış modellerinin öğretilmesi, siber güvenlik stratejilerinin etkinliğini artırır.

3.4.2. Sosyal Mühendislik Saldırıları

İnsan unsuru, sosyal mühendislik saldırılarının önlenmesinde de kritik bir role sahiptir. "Sosyal mühendislik, saldırganların hedeflerine ulaşmak için insan psikolojisini kullanarak bilgi elde etmeye çalıştığı bir saldırı türüdür"

(Hadnagy, 2010, s. 22). Eğitim programları, çalışanların bu tür saldırılara karşı daha dirençli hale gelmesini sağlar.

3.4.3. Hedefe Yönelik Eğitimler

Eğitim programlarının tasarımında, farklı düzeylerde ve roller için özelleştirilmiş eğitimlerin önemi büyüktür. "Her seviyede çalışan için uygun eğitim programları, siber güvenlik politikalarının etkinliğini artırır" (Agaba, 2020).

3.4.4. Sürekli Eğitim ve Güncelleme

Siber tehditlerin sürekli değişmesi nedeniyle, eğitim programlarının da sürekli güncellenmesi gerekmektedir. "Siber güvenlik eğitimleri, düzenli aralıklarla yenilenmeli ve güncel tehditlere karşı korunma yöntemleri içermelidir" (Vasileiou & Furnell, 2019, s. 158).

3.4.5. Güvenlik Kültürünün Oluşturulması

İnsan kaynakları politikaları, güvenlik kültürünün oluşturulmasında önemli bir rol oynar. "Güvenlik kültürü, çalışanların siber güvenlik konusundaki tutum ve davranışlarını şekillendirir" (Schlienger & Teufel, 2003). Bu kültür, organizasyon genelinde güvenlik bilincinin artırılmasını sağlar.

3.4.6. Motivasyon ve Katılım

Çalışanların siber güvenlik eğitimlerine aktif katılımı, motivasyon ve ödüllendirme sistemleri ile desteklenmelidir. "Motivasyon artırıcı stratejiler, çalışanların siber güvenlik eğitimlerine olan ilgisini ve katılımını artırır" (Ifinedo, 2012, s. 89).

Siber güvenlik eğitimi politikalarında insan unsurunun önemi, güvenlik bilincinin artırılması, sosyal mühendislik saldırılarının önlenmesi ve güvenlik kültürünün oluşturulması gibi birçok alanda kendini göstermektedir. Bu nedenle, eğitim programlarının tasarımında insan faktörünün dikkate alınması, siber güvenlik stratejilerinin başarısını artıracaktır.

4. TÜRKİYE'DE SİBER GÜVENLİK: POLİTİKASI, EĞİTİM POLİTİKASI VE EĞİTİM PROGRAMLARI

Türkiye'de siber güvenlik politikası ve eğitimi, ülkenin dijitalleşme sürecinde önemli bir rol oynamaktadır. Hızla gelişen teknoloji ve artan dijitalleşme, siber tehditlere karşı daha güçlü ve etkili önlemler alınmasını gerektirmektedir. Bu bağlamda, Türkiye, siber güvenlik politikalarını güçlendirmekte ve bu alanda kapsamlı eğitim programları geliştirmektedir. Türkiye'nin siber güvenlik stratejisi, ulusal güvenliğin korunması, kritik altyapıların güvenliğinin sağlanması ve bireylerin siber güvenlik konusunda bilinçlendirilmesi üzerine odaklanmaktadır. Yüksek Öğretim Kurumu (YÖK) bünyesindeki Üniversitelerden bazıları, siber güvenlik alanında uzmanlaşmış bireyler yetiştirmek amacıyla lisans ve lisansüstü programlar sunmakta, pratik uygulamalarla desteklenen teorik eğitimler vermektedir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi bünyesindeki Siber Güvenlik Daire Başkanlığı koordinasyonunda yine YÖK bünyesindeki bazı üniversitelerde siber güvenlik alanında ön lisans programı açılması da salık verilmiştir ve bu programlarda eğitim öğretime başlanmıştır. Tabii ki eğitim denince akla ilk gelen kurum olan Milli Eğitim Bakanlığı (MEB) bünyesinde bilişim teknolojileri dersleri, sosyal bilimler dersleri ve medya okuryazarlığı gibi derslerde bilişim güvenliği dijital yurttaşlık gibi başlıklarda siber güvenliğe dair kazanımlara yer verilmektedir. Yine MEB bünyesinde siber güvenlik alanına odaklı bir meslek lisesi kurulmuş ve çalışmalarını sürdürmektedir ayrıca yeni teknik liselerin de bu alanda tahsisleri gündemdedir. Ayrıca, TÜBİTAK ve Hava Elektronik Sanayi (HAVELSAN), Askeri Elektronik Sanayi (ASELSAN), Bilgi Teknolojileri ve İletişim Kurumu (BTK), Savunma Sanayii Başkanlığı (SSB) ve bünyesindeki Siber Güvenlik Kümelenmesi, Türk Silahlı Kuvvetler (TSK), Emniyet Genel Müdürlüğü (EGM) gibi kurumlar, siber güvenlik eğitimine katkıda bulunarak ulusal kapasitenin artırılmasına yardımcı olmaktadır. Türkiye'de siber güvenlik politikası ve eğitiminin güçlendirilmesi hem ulusal güvenliğin sağlanması hem de küresel siber tehditlere karşı etkin bir duruş sergilenmesi açısından büyük önem taşımaktadır.

Siber güvenlik, dijital çağın getirdiği en kritik disiplinlerden biri olarak, özellikle Türkiye'de eğitim alanında hızla gelişen ve önem kazanan bir alan

haline gelmiştir. Bu bağlamda, siber güvenlik eğitimine dair temel kavramlar, hem öğrencilerin hem de profesyonellerin bu alandaki bilgi ve becerilerini artırmak için kilit rol oynamaktadır. Temel kavramlar arasında; bilgi güvenliği, ağ güvenliği, siber tehditler ve saldırı türleri, kriptografi, siber güvenlik politikaları ve düzenlemeleri yer almaktadır. Bu kavramlar, siber güvenlik eğitiminin temelini oluşturarak, öğrencilere teorik bilgi sağlamanın yanı sıra, pratik uygulamalarla da desteklenerek onların gerçek dünya problemlerine karşı donanımlı hale gelmelerini amaçlamaktadır. Türkiye'de üniversiteler ve çeşitli eğitim kurumları, bu temel kavramları müfredatlarına entegre ederek, ülkenin siber güvenlik alanındaki yetkinliğini artırmayı hedeflemektedir. Bu sayede, Türkiye'nin siber güvenlik ekosistemi güçlenmekte ve küresel düzeyde rekabet edebilir bir konuma gelmektedir.

4.1. TÜRKİYE'DE SİBER GÜVENLİK POLİTİKASI

Türkiye, siber güvenlik alanında son yıllarda önemli adımlar atmış bir ülkedir. Siber tehditlerin artmasıyla birlikte, ulusal güvenliğin sağlanması amacıyla kapsamlı siber güvenlik stratejileri geliştirilmiştir. 2013 senesinde duyurulan Ulusal Siber Güvenlik Stratejisi ve sonrasında 2014-2016 Eylem Planı, Türkiye'nin bu alandaki ilk büyük adımlarını oluşturmuştur (Karataş, 2020). Bu strateji, siber tehditlere karşı ulusal güvenliğin artırılmasını hedefleyen çeşitli önlemler ve politikalar içermektedir. Özellikle, devlet kuruluşları ve özel sektör tarafında iş birliğinin artırılması ve siber güvenlik farkındalığının yaygınlaştırılması bu politikanın temel unsurlarındandır.

Türkiye'nin siber güvenlik politikaları, uluslararası gelişmeler ve tehditlerin analiz edilmesiyle sürekli olarak güncellenmektedir. Özellikle, NATO ve Avrupa Birliği gibi uluslararası kuruluşlarla iş birliği yapılarak, küresel siber tehditlere karşı ortak stratejiler geliştirilmektedir (European Union External Action Service, 2023). Ayrıca, Türkiye'de siber güvenlik özelinde bilinç geliştirmek ve eğitim programlarını yaygınlaştırmak amacıyla çeşitli kampanyalar ve projeler yürütülmektedir (International Telecommunication Union, 2014). Bu girişimlerin yanı sıra, Türkiye'nin siber güvenlik alanındaki mevzuatı da sürekli olarak yenilenmekte ve güçlendirilmektedir.

Siber güvenlik alanında Türkiye'nin stratejileri, sadece savunma mekanizmaları kurmakla sınırlı değildir. Aynı zamanda, siber tehditleri önceden tespit etmek ve bu tehditlere karşı proaktif önlemler almak da bu stratejilerin bir parçasıdır. Bu bağlamda, Türkiye'nin siber güvenlik politikaları, teknolojik altyapının güçlendirilmesi ve insan kaynağının geliştirilmesi gibi alanlarda da yoğunlaşmaktadır (Daily Sabah, 2023). Bu stratejiler, Türkiye'nin siber güvenlik alanında ulusal ve de uluslararası düzeyde etkin bir oyuncu olmasını sağlamaktadır.

4.1.1. 2014-2016 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Türkiye'nin siber güvenlik politikalarının temelini oluşturan bu eylem planı, ülkenin siber tehditlere karşı ilk büyük adımlarını temsil etmektedir (Insight Turkey, 2022). Planın hedefleri arasında, kritik altyapıların korunması, siber saldırılara karşı etkin savunma mekanizmalarının kurulması ve siber güvenlik farkındalığının artırılması yer alır (Karataş, 2020). Ayrıca, ulusal ve uluslararası düzeyde iş birliğinin güçlendirilmesi gerektiği vurgulanmıştır (International Telecommunication Union, 2014). Bu kapsamda Türkiye, AB ve NATO gibi kuruluşlarla iş birliği yaparak, ortak stratejiler geliştirmektedir (European Union External Action Service, 2023).

4.1.2. Türkiye'de Siber Güvenlik: Tehditler ve Önlemler

Siber tehditler, ulusal güvenlik açısından büyük riskler taşımaktadır. Türkiye, bu tehditlere karşı çeşitli savunma mekanizmaları geliştirerek, siber güvenlik alanında proaktif bir strateji benimsemiştir (Özker, 2022). Bu strateji, siber tehdit istihbaratının toplanması, bilgi güvenliği mimarisinin oluşturulması ve acil durum müdahale ekiplerinin kurulması gibi önlemleri içermektedir (Halisdemir, 2021). Ayrıca, siber güvenlik bilincini artırmak amacıyla eğitim programları ve kampanyalar düzenlenmekte, mevzuat sürekli olarak yenilenmektedir (EC-Council, 2024).

4.1.3. Türkiye'nin Siber Güvenlik Stratejileri ve Uygulamaları

Türkiye'nin siber güvenlik stratejileri, ulusal güvenliğin sağlanmasına yönelik çeşitli önlemleri kapsamaktadır. Bu stratejiler arasında, siber tehdit istihbaratı toplama, bilgi güvenliği mimarisi oluşturma ve acil durum müdahale

ekiplerinin kurulması yer alır (Halisdemir, 2021). Ayrıca, devlet ve özel sektör iş birliğiyle siber tehditlere karşı etkili bir savunma sağlanmaktadır. Türkiye, AB ve NATO gibi kuruluşlarla iş birliği yaparak, küresel siber tehditlere karşı ortak stratejiler geliştirmektedir (Halisdemir, 2021). Siber güvenlik bilincini artırmak amacıyla eğitim programları ve projeler de yürütülmektedir (EC-Council, 2024).

4.1.4. Özel Sektör ve Kamu Kurumları Arasında Siber Güvenlik İş Birliği

Siber güvenlik stratejilerinin başarılı bir şekilde uygulanması için özel sektör ve kamu kurumları arasında iş birliği kritik öneme sahiptir. Türkiye, bu iş birliğini artırmak amacıyla bilgi paylaşımını teşvik eden platformlar oluşturmuş ve ortak projeler geliştirmiştir (International Institute for Strategic Studies, 2023). Bu iş birliği, siber tehditlere karşı etkin bir savunma sağlamakta ve siber güvenlik farkındalığını artırmaktadır. Ayrıca, yenilikçi çözümler ve teknolojiler geliştirilmesi teşvik edilmektedir (Halisdemir, 2021).

4.2. TÜRKİYE'DE SİBER GÜVENLİK EĞİTİMİ POLİTİKASI

Siber güvenlik, günümüzde ulusal güvenliğin ayrılmaz bir parçası haline gelmiştir. Teknolojinin hızla gelişmesiyle birlikte siber tehditler de artmakta ve bu tehditlere karşı korunmak için siber güvenlik eğitimi büyük önem taşımaktadır. Bilgi güvenliğinin sağlanması, kullanıcıların farkındalığının artırılması ile güçlenir (Çakır & Taşer, 2023).

Modern dünya, bilgi teknolojilerinin hızlı gelişimi ve internetin yaygın kullanımıyla birlikte, bireylerin ve kurumların siber tehditlere karşı daha savunmasız hale gelmesine neden olmuştur. Siber saldırılar, kişisel bilgilerden ticari sırların çalınmasına kadar geniş bir yelpazede zararlar verebilir. Bu nedenle, siber güvenlik eğitimi sadece teknik becerilerle sınırlı kalmamalı, aynı zamanda etik, hukuk ve sosyal boyutları da kapsamalıdır. Siber güvenlik eğitiminin amacı, bireylerin ve kurumların bu tehditlere karşı bilinçlenmesini ve etkin savunma stratejileri geliştirmesini sağlamaktır (Çakır & Taşer, 2023).

Siber güvenlik eğitiminde dikkat edilmesi gereken bir diğer önemli nokta, eğitimin sadece teknik bilgi ile sınırlı kalmamasıdır. Siber güvenlik eğitimi,

bireylerin etik kuralları, hukuki düzenlemeleri ve sosyal sorumlulukları öğrenmesini de içermelidir. Özellikle siber etik, bireylerin çevrimiçi ortamda doğru ve güvenli davranışlar sergilemesi için kritik bir öneme sahiptir. Siber etik, kişisel verilerin korunması, dijital vatandaşlık ve çevrimiçi davranış kuralları gibi konuları kapsar (Kurnaz & Önen, 2019).

Siber güvenlik eğitimi, aynı zamanda siber suçların önlenmesi ve siber terörizme karşı korunma stratejilerinin geliştirilmesi açısından da büyük bir öneme sahiptir. Siber suçlar ve siber terörizm, ülkelerin ekonomik ve ulusal güvenliğini tehdit eden ciddi sorunlardır. Bu nedenle, siber güvenlik eğitimi, siber suçların ve siber terörizmin önlenmesi ve bu tehditlere karşı etkin savunma stratejilerinin geliştirilmesi açısından kritik bir rol oynamaktadır (Çakır & Taşer, 2023).

Siber güvenlik eğitimi, dijital dünyada güvenliği sağlamak için kritik öneme sahiptir. Türkiye'de siber güvenlik eğitimi, kamu kurumları, üniversiteler ve özel sektör tarafından sağlanan çeşitli programlar ve sertifikasyonlar aracılığıyla verilmektedir. Bu eğitim programları, öğrencileri ve profesyonelleri siber tehditlere karşı savunma mekanizmaları geliştirme konusunda donatmayı amaçlamaktadır. Türkiye'deki siber güvenlik eğitimi, uluslararası standartlara uyumlu müfredatlarla desteklenmektedir ve bu alandaki yetkinliği artırmayı hedeflemektedir (Halisdemir, 2021).

Türkiye'de siber güvenlik alanında lise düzeyinde mesleki alan olarak başlamak üzere üniversite düzeyinde de lisans, yüksek lisans ve doktora programları sunulmaktadır. Ayrıca, TÜBİTAK ve BTK gibi kamu kurumları tarafından sunulan sertifikasyon programları, profesyonellerin siber güvenlik becerilerini geliştirmelerine yardımcı olmaktadır (CoHE, 2023). Özel sektör de bu alanda önemli katkılar sunmakta, özellikle büyük teknoloji firmaları ve güvenlik şirketleri, çalışanlarına yönelik kapsamlı siber güvenlik eğitimleri düzenlemektedir (Spoclearn, 2024).

Siber güvenlik eğitimi, sadece teknik becerilerin geliştirilmesinin yanı sıra; stratejik düşünme, risk yönetimi ve etik konularını da içermektedir. Bu kapsamlı yaklaşım, siber güvenlik profesyonellerinin geniş bir perspektif kazanmalarını sağlamaktadır (Cyber Security Educational Curriculums in

Turkey, 2016). Ayrıca, Türkiye'deki siber güvenlik eğitim programları, öğrencilere ve profesyonellere pratik deneyimler sunmak için laboratuvar çalışmaları ve staj imkânları gibi uygulamalı öğrenme fırsatları da sunmaktadır. Eğitim programlarının yanı sıra, farkındalık yaratma kampanyaları ve seminerler de siber güvenlik alanında bilinç düzeyini artırmayı hedeflemektedir. Bu tür etkinlikler, öğrencilerin olduğu kadar profesyonellerin de siber güvenlik konusunda güncel bilgiye sahip olmalarını sağlamaktadır.

4.2.1. Türkiye'de Siber Güvenlik Eğitiminin Durumu ve Önemi

Günümüzde dijitalleşmenin hız kazanmasıyla birlikte, siber güvenlik kavramı her zamankinden daha büyük bir önem kazanmıştır. Bilgi ve iletişim teknolojilerinin gelişimi, bireylerin ve kurumların verilerini çevrimiçi ortamlarda saklamasını yaygınlaştırmış, bu da siber tehditlerin artmasına yol açmıştır. Türkiye, siber güvenlik alanında kendini geliştirmek ve bu tehditlere karşı etkin önlemler alabilmek adına, eğitim kurumlarında siber güvenlik eğitiminin yaygınlaştırılmasına büyük önem vermektedir. Türk üniversiteleri, bu alanda nitelikli uzmanlar yetiştirmek amacıyla çeşitli lisans, yüksek lisans ve sertifika programları sunmaktadır. Bu eğitimler, teorik bilgilerin yanı sıra pratik uygulamalarla da desteklenerek, öğrencilerin gerçek dünya siber güvenlik sorunlarına hazırlıklı olmalarını sağlamaktadır. Türkiye'nin siber güvenlik alanındaki insan kaynağını güçlendirmek ve küresel arenada rekabet edebilir bir konuma gelmek için siber güvenlik eğitiminin yaygınlaştırılması ve kalitesinin artırılması kritik bir rol oynamaktadır.

4.2.2. Türkiye'de Siber Güvenlik Eğitiminin Tarihsel Gelişimi

Türkiye'de siber güvenlik eğitimi, henüz istenilen düzeyde olmasa da gelişim göstermektedir. Ulusal strateji ve eylem planları, bu alandaki eksiklikleri gidermek için önemli adımlar içermektedir. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (2020) tarafından yayımlanan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023" bu bağlamda kritik bir öneme sahiptir. Eğitim kurumlarında siber güvenlik derslerinin müfredata dahil edilmesi ve farkındalık çalışmalarının artırılması gerekmektedir (Dijital Dönüşüm Ofisi, 2020).

Türkiye’de siber güvenlik eğitiminin tarihsel gelişimi, 1990'lı yılların sonlarından itibaren başlamıştır. İlk olarak büyük üniversiteler ve askeri okullar, siber güvenlik konusunda dersler ve araştırma projeleri başlatmıştır. Ancak bu eğitimler, genellikle teknik bilgiyle sınırlı kalmış ve geniş kitlelere ulaşamamıştır. 2000'li yıllarda, siber tehditlerin artması ve devlet kurumlarının bu alandaki farkındalığının artmasıyla birlikte, siber güvenlik eğitimi daha sistematik hale gelmiştir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planları, bu sürecin bir parçası olarak geliştirilmiş ve eğitim kurumlarına rehberlik etmiştir (Kurnaz & Önen, 2019).

2010'lu yıllarda, ulusal ve uluslararası siber güvenlik stratejileri ve eylem planları kapsamında, siber güvenlik eğitimi alanında önemli adımlar atılmıştır. Bu dönemde, devlet kurumları, üniversiteler ve özel sektör arasında iş birlikleri artırılarak, siber güvenlik eğitiminin kapsamı genişletilmiştir (Özker, 2022).

Bu gelişmelerin ışığında, Türkiye'de siber güvenlik eğitiminin tarihsel süreçteki önemli adımlarını daha ayrıntılı incelemek gerekmektedir. İlk olarak, üniversitelerdeki siber güvenlik eğitim programlarının evrimi ve bu programların içeriği incelenmelidir. Ayrıca, askeri okulların ve devlet kurumlarının siber güvenlik eğitimine katkıları değerlendirilmelidir (Özker, 2022).

Siber güvenlik eğitiminin tarihsel gelişimi, Türkiye'nin siber güvenlik alanındaki eksikliklerini gidermek ve bu alanda daha yetkin bireyler yetiştirmek için atılan adımları kapsamaktadır. Bu bağlamda, siber güvenlik eğitiminin tarihi süreçteki önemli dönüm noktaları ve bu dönüm noktalarının eğitime etkileri değerlendirilmelidir (Dijital Dönüşüm Ofisi, 2020, s. 28).

4.2.3. Türkiye’de Güncel Durum ve Mevcut Uygulamalar

Dünya genelinde birçok ülke, siber güvenlik eğitimine büyük önem vermekte ve çeşitli stratejiler geliştirmektedir. Özellikle ABD, İngiltere, Almanya gibi ülkelerde siber güvenlik eğitimi konusunda ciddi yatırımlar yapılmaktadır. Bu ülkelerde, siber güvenlik eğitimi hem akademik düzeyde hem de kamu ve özel sektör iş birliğiyle yürütülmektedir. Türkiye’nin de bu örneklerden ilham alarak kendi siber güvenlik eğitim stratejilerini geliştirmesi önem arz etmektedir (Özker, 2022).

Türkiye'de siber güvenlik eğitimi, çeşitli üniversitelerde ve meslek yüksekokullarında dersler ve sertifika programları şeklinde verilmektedir. Ayrıca, özel sektör ve kamu kurumları, çalışanlarına yönelik siber güvenlik eğitimleri düzenlemektedir. Bu eğitimler, genellikle teknik beceriler üzerine odaklanmakta olup, kullanıcı farkındalığını artırmayı hedeflemektedir. Ancak, bu eğitimlerin yeterli düzeyde olmadığı ve daha kapsamlı programlara ihtiyaç duyulduğu belirtilmektedir (Dijital Dönüşüm Ofisi, 2020).

Türkiye'de siber güvenlik eğitimi konusunda atılan adımlar, özellikle üniversiteler ve meslek yüksekokulları düzeyinde önemli ilerlemeler sağlamıştır. Ancak, bu alandaki eğitimlerin etkinliğini artırmak için daha fazla kaynak ve destek sağlanması gerekmektedir. Özellikle kırsal bölgelerdeki okulların teknoloji altyapısının iyileştirilmesi ve öğretmenlerin siber güvenlik konularında sürekli eğitim alması önemlidir (Dijital Dönüşüm Ofisi, 2020).

Türkiye'de siber güvenlik eğitimi ve mevcut uygulamaları daha ayrıntılı incelemek için, belirli üniversitelerde ve meslek yüksekokullarında verilen siber güvenlik derslerinin içeriği, eğitim materyalleri ve öğretim yöntemleri değerlendirilmelidir. Ayrıca, özel sektör ve kamu kurumlarının siber güvenlik eğitimlerine yönelik çabaları ve bu eğitimlerin etkinliği incelenmelidir (Çakır & Taşer, 2023).

Türkiye'de siber güvenlik eğitiminin geliştirilmesi için, mevcut uygulamaların değerlendirilmesi ve bu alanda daha fazla kaynağın sağlanması gerekmektedir. Ayrıca, siber güvenlik eğitiminde kullanılan materyallerin güncellenmesi ve öğretim yöntemlerinin iyileştirilmesi önemlidir. Bu sayede, öğrencilere ve çalışanlara daha etkili bir eğitim sunulabilir (Özker, 2022).

Türkiye'de siber güvenlik eğitiminin mevcut durumu ve ihtiyaçlarını daha ayrıntılı incelemek için, çeşitli üniversitelerde ve meslek yüksekokullarında verilen derslerin içeriği ve bu derslerin öğrencilere kazandırdığı beceriler değerlendirilmelidir. Ayrıca, siber güvenlik eğitimi konusunda atılan adımların etkinliği ve bu adımların eğitim kurumlarına ve öğrencilere etkileri incelenmelidir (Dijital Dönüşüm Ofisi, 2020).

4.3.TÜRKİYE'DE BİLİŞİM TEKNOLOJİLERİ EĞİTİMİ

Türkiye'de bilişim teknolojileri eğitimi, dijital dönüşüm sürecinin hızlanmasıyla birlikte giderek daha önemli bir hale gelmiştir. Bilgi ve iletişim teknolojilerinin hızla gelişmesi, bireylerin ve kurumların bu alanda yetkinlik kazanmasını zorunlu kılmaktadır. Bu gerekliliği karşılamak amacıyla, Türkiye'de eğitim kurumları, bilişim teknolojileri müfredatlarını güncelleyerek öğrencilere çağdaş bilgi ve beceriler kazandırmayı hedeflemektedir. Ortaokuldan üniversiteye kadar çeşitli düzeylerde sunulan bilişim teknolojileri dersleri, öğrencilere hem teorik bilgiler hem de pratik uygulama fırsatları sunarak onların dijital dünyada etkin bir şekilde var olmalarını sağlamaktadır. Bilişim teknolojileri eğitimi, öğrencilere analitik düşünme, problem çözme ve yenilikçi çözümler geliştirme gibi önemli beceriler kazandırarak, siber güvenlik alanında da sağlam bir temel oluşturmaktadır. Siber güvenlik eğitimine geçişte kritik bir rol oynayan bilişim teknolojileri dersleri, öğrencilere bilgi güvenliği, ağ güvenliği ve siber tehditlerle başa çıkma konularında gerekli altyapıyı sunmaktadır.

4.3.1. Türkiye'de Bilişim Teknolojileri Eğitiminde Mevcut Durum ve İhtiyaçlar

Türkiye'de bilişim teknolojileri eğitimi, özellikle son yıllarda hızla gelişim göstermiştir. MEB müfredatında bilişim teknolojileri dersleri önemli bir yer tutmakta ve bu dersler, öğrencilere temel bilgisayar becerilerinin yanı sıra internet güvenliği ve veri koruma gibi konuları da öğretmektedir. Ancak, siber güvenlik eğitimi henüz bu müfredat içinde yeterince yer bulamamaktadır (Özker, 2022).

Türkiye'de bilişim teknolojileri eğitiminin mevcut durumu, çeşitli düzeylerdeki eğitim kurumlarında verilen dersler ve programlar aracılığıyla değerlendirilmelidir. İlkokuldan üniversiteye kadar, bilişim teknolojileri dersleri öğrencilere temel bilgisayar becerileri ve bilgi güvenliği konularını öğretir. Ancak, siber güvenlik eğitimi henüz bu müfredat içinde yeterince yer bulamamaktadır. Bu durum, siber tehditlere karşı korunma bilincinin yeterince gelişmemesine neden olabilir (Çakır & Taşer, 2023).

Bilişim teknolojileri eğitiminin etkinliği, öğretim materyallerinin güncelliği ve öğretmenlerin bilgi düzeyi ile doğrudan ilişkilidir. Öğrencilere sağlanan eğitim materyalleri, siber tehditlere karşı korunma yöntemlerini içermeli ve güncel teknolojik gelişmeleri takip etmelidir. Öğretmenlerin de bu konularda sürekli eğitim alması ve mesleki gelişimlerini sürdürmeleri gerekmektedir (Çakır & Taşer, 2023).

Türkiye'de bilişim teknolojileri alanında ilk formal zorunlu ders "Bilişim Teknolojileri ve Yazılım Dersi (BTYD)" adıyla ortaokul 5. sınıftan itibaren haftada 2 saat olarak müfredata dâhil edilmiştir. Ancak, ortaokullarda bilişim teknolojileri eğitimi için uygun öğrenme ortamlarının oluşturulmasında gecikmeler yaşanmaktadır. Bilişim teknolojilerindeki hızlı gelişmelerin eğitim sistemine etkin bir şekilde entegre edilebilmesi ve bu kazanımların öğrencilere aktarılabilmesi için eğitim ortamlarının da aynı hızla güncellenebilir, modern ve öğrencilere üretim odaklı öğrenme imkânı tanıyan donanımlara sahip olması gerekmektedir (Eskici, 2019). Siber güvenlik alanında eğitim doğru ve verimli bilişim teknolojileri eğitimi ortamlarının sağlanabildiği oranda başarılı olabilecektir.

Bilişim teknolojileri eğitiminin mevcut durumunu daha ayrıntılı değerlendirmek için, farklı eğitim seviyelerindeki müfredatlar ve bu müfredatların siber güvenlik konularını nasıl ele aldığı incelenmelidir. Ayrıca, öğretmenlerin siber güvenlik konularındaki bilgi düzeyi ve bu konularda aldıkları eğitimler değerlendirilmelidir (Gündüz ve Daş, 2022).

Türkiye'de bilişim teknolojileri eğitimi, sadece teknik becerilerle sınırlı kalmamalı, aynı zamanda öğrencilerin siber tehditlere karşı bilinçlenmesini sağlamalıdır. Bu nedenle, bilişim teknolojileri eğitimi müfredatına siber güvenlik derslerinin eklenmesi ve bu derslerin etkin bir şekilde verilmesi önemlidir (Çakır & Taşer, 2023).

Bilişim teknolojileri eğitiminin mevcut durumu ve bu eğitimin siber güvenlik eğitimi ile entegrasyonunu daha ayrıntılı incelemek için, eğitim kurumlarındaki derslerin içeriği ve bu derslerin öğrencilere kazandırdığı beceriler değerlendirilmeli; ayrıca, öğretmenlerin siber güvenlik konularındaki bilgi

düzeyi ve bu konularda aldıkları eğitimler incelenmelidir (Gündüz ve Daş, 2022).

4.3.2. Türkiye'de Bilişim Teknolojileri Eğitimi ve Siber Güvenlik

Türkiye'deki birçok üniversite, bilişim teknolojileri ve bilgisayar mühendisliği programları sunmaktadır. Bu programlar, öğrencilere teorik bilgi ve pratik beceriler kazandırmayı hedeflemektedir. Özellikle büyük üniversiteler, siber güvenlik konusunda uzmanlaşmış bölümler ve laboratuvarlar kurmuş durumdadır. Örneğin, İstanbul Teknik Üniversitesi (İTÜ), siber güvenlik alanında ileri düzey araştırmalar ve projeler yürütmektedir. Bu tür programlar, öğrencilerin siber güvenlik alanında yetkinlik kazanmaları için önemlidir (Çakır & Taşer, 2023).

Bilişim teknolojileri eğitimi, öğrencilere temel bilgisayar becerileri ve bilgi güvenliği konularını öğretirken, siber güvenlik eğitimi bu bilgileri derinleştirir ve öğrencilere siber tehditlere karşı korunma stratejilerini öğretir. Bu iki eğitim alanı arasındaki ilişki, öğrencilere pratik ve teorik bilgi kazandırarak, onları siber tehditlere karşı daha donanımlı hale getirir. Bu nedenle, bilişim teknolojileri eğitimi ile siber güvenlik eğitimi arasında sıkı bir entegrasyon sağlanmalıdır (Çakır & Taşer, 2023).

Bilişim teknolojileri eğitimi ile siber güvenlik eğitimi arasındaki ilişkiyi daha ayrıntılı incelemek için, üniversitelerdeki programların müfredatları ve bu müfredatların siber güvenlik konularını nasıl ele aldığı değerlendirilmeli; ayrıca, öğrencilere sağlanan pratik eğitim fırsatları ve bu fırsatların etkinliği incelenmelidir (Özker, 2022).

Bilişim teknolojileri eğitiminin etkinliğini artırmak için, öğrencilere sağlanan eğitim materyallerinin güncellenmesi ve öğretim yöntemlerinin iyileştirilmesi önemlidir. Bu sayede, öğrencilere daha kapsamlı ve etkili bir eğitim sunulabilir (Gündüz ve Daş, 2022).

4.3.2.1.Türkiye'de Siber Güvenlik Eğitimi ile Bilişim Teknolojileri Eğitimi Arasındaki İlişki

Siber güvenlik ve bilişim teknolojileri eğitimi, modern bilgi çağında birbirini tamamlayan iki kritik disiplindir. Bilişim teknolojileri eğitimi, öğrencilere

bilgisayar bilimi, yazılım geliştirme, ağ yönetimi ve veri analizi gibi temel bilgi ve becerileri kazandırırken, siber güvenlik eğitimi bu bilgi ve becerilerin güvenli bir şekilde uygulanmasını sağlar. Bu entegrasyon, dijital dünyada etkin ve güvenli bilgi yönetimi için hayati önem taşır. Siber güvenlik eğitimi, teknik bilgi ve becerilerin güvenli bir şekilde uygulanmasına odaklanarak, bireylerin siber tehditlere karşı korunma stratejilerini geliştirmelerini sağlar (Çakır & Taşer, 2023).

Bilişim teknolojileri eğitimi, öğrencilere temel bilgisayar becerileri kazandırırken, siber güvenlik eğitimi bu bilgileri derinleştirir ve pratik çözümler sunar. Bu eğitimler, siber tehditlere karşı etkin savunma stratejileri geliştirmek için gereklidir. Türkiye'deki eğitim kurumlarının, siber güvenlik eğitimine daha fazla önem vererek müfredatlarını güncellemeleri ve öğrencilere kapsamlı bir eğitim sunmaları gerekmektedir (Çakır & Taşer, 2023; Özker, 2022).

Siber güvenlik eğitimi ile bilişim teknolojileri eğitimi arasındaki entegrasyon, öğrencilerin hem teorik bilgi hem de pratik beceriler kazanmalarını sağlar. Bu eğitimler, öğrencilerin siber güvenlik konusunda bilinçlenmesini ve bu alanda kariyer yapma isteklerini artırır. Ayrıca, bu tür bir eğitim, ülkenin siber güvenlik kapasitesini artırarak ulusal güvenliği güçlendirir (Çakır & Taşer, 2023).

4.3.2.2. Türkiye'de Siber Güvenlik Eğitiminde Bilişim Teknolojileri Kullanımı

Siber güvenlik eğitiminde bilişim teknolojilerinin kullanımı, eğitimin etkinliğini artırmak için önemlidir. Öğrencilere sağlanan bilgisayar laboratuvarları ve simülasyon ortamları, onların siber tehditleri tespit etme ve bu tehditlere karşı savunma stratejileri geliştirme becerilerini artırmaktadır. Ayrıca, sanal gerçeklik (VR) ve artırılmış gerçeklik (AR) gibi teknolojiler, öğrencilere siber saldırı senaryolarını simüle etme ve bu senaryolar üzerinde çalışarak pratik beceriler kazandırma imkanı sunmaktadır (Çakır & Taşer, 2023).

Bilişim teknolojileri, siber güvenlik eğitiminde kullanılan araçlar ve yöntemler arasında önemli bir yer tutmaktadır. Bilgisayar laboratuvarları ve simülasyon

ortamları, öğrencilere siber saldırıları tespit etme ve bu saldırılara karşı savunma stratejileri geliştirme becerileri kazandırmaktadır. Ayrıca, sanal gerçeklik ve artırılmış gerçeklik teknolojileri, öğrencilere siber saldırı senaryolarını simüle etme ve bu senaryolar üzerinde çalışarak pratik beceriler kazandırma imkânı sunmaktadır (Çakır & Taşer, 2023).

4.4.TÜRKİYE'DE SİBER GÜVENLİK EĞİTİM PROGRAMLARI

Türkiye'de siber güvenlik eğitimi, üniversitelerin siber güvenlik, yazılım mühendisliği, bilgi güvenliği ve bilgisayar mühendisliği bölümlerinde yoğunlaşmaktadır. Bu bölümler, öğrencilerin siber tehditleri anlama ve bu tehditlere karşı etkili savunma mekanizmaları geliştirme becerilerini kazanmalarını sağlamaktadır (Daily Sabah, 2023). Üniversitelerde sunulan programlar, temel bilgisayar bilimi derslerinden ileri düzey siber güvenlik konularına kadar geniş bir müfredat içermektedir (CoHE, 2023). Ayrıca, bu programlar uluslararası akreditasyonlara sahip olup, mezunların global standartlara uygun bilgi ve becerilerle donatılmasını sağlamaktadır (Daily Sabah, 2023).

TÜBİTAK ve BTK gibi kamu kurumları, siber güvenlik alanında çeşitli sertifikasyon programları sunmaktadır. Bu programlar, profesyonellerin siber güvenlik kabiliyetlerinin geliştirmelerine katkı sunmakta ve kariyerlerinde ilerlemelerini sağlamaktadır (TÜBİTAK, 2023). TÜBİTAK'ın düzenlediği Siber Güvenlik Yaz Okulu, bu mecrada eğitim almak isteyen profesyonellere ve öğrencilere geniş kapmsamlı bir eğitim programı sunmaktadır (TÜBİTAK, 2023). BTK'nın Siber Yıldız Programı ise, siber güvenlik uzmanları yetiştirmek amacıyla çeşitli eğitimler ve yarışmalar düzenlemektedir (CoHE, 2023).

Özel sektör de siber güvenlik eğitimine önemli katkılar sunmaktadır. Büyük teknoloji firmaları ve güvenlik şirketleri, çalışanlarına yönelik kapsamlı siber güvenlik eğitim programları düzenlemekte ve bu alanda uzmanlaşmalarını sağlamaktadır (Spoclearn, 2024). Ayrıca, özel sektör tarafından sunulan sertifikasyon programları, profesyonellerin siber güvenlik alanındaki yetkinliklerini artırmalarına yardımcı olmaktadır. Örneğin, SANS Institute gibi uluslararası tanınmış kuruluşlar tarafından sunulan sertifikasyonlar,

profesyonellerin global standartlarda bilgi ve beceri kazanmalarını sağlamaktadır (SANS Institute, 2024).

Bu kapsamlı eğitim programları, siber güvenlik uzmanlarının yetkinliklerini artırmakta ve onların sektördeki en son gelişmelerden haberdar olmalarını sağlamaktadır. Ayrıca, bu programlar sayesinde siber güvenlik alanında sürekli öğrenme ve gelişim teşvik edilmektedir (Daily Sabah, 2023). Türkiye'de siber güvenlik eğitim programları ve sertifikasyonlar, hem teknik hem de stratejik becerilerin geliştirilmesine katkıda bulunmaktadır.

4.4.1. Üniversitelerde Siber Güvenlik Eğitim Müfredatları

Türkiye'deki üniversiteler, siber güvenlik alanında kapsamlı ve güncel eğitim müfredatları sunmaktadır. Bilgisayar mühendisliği ve bilgi güvenliği bölümleri, siber güvenlik alanında uzmanlaşmayı sağlayan dersler ve programlar içermektedir (Daily Sabah, 2023). Bu programlar, temel bilgisayar bilimi derslerinden başlayarak, ağ güvenliği, kriptografi, etik hacking ve siber tehdit istihbaratı gibi ileri düzey konuları kapsamaktadır (Aldirasa, 2024). Ayrıca, üniversiteler, öğrencilere pratik deneyimler sunmak amacıyla laboratuvar çalışmaları ve staj imkânları sağlamaktadır (Daily Sabah, 2023).

Üniversitelerde sunulan siber güvenlik eğitim müfredatları, öğrencilere geniş bir perspektif kazandırmayı hedeflemektedir. Bu müfredatlar, teknik becerilerin yanı sıra, stratejik düşünme, risk yönetimi ve etik konularını da içermektedir. Böylece, öğrenciler siber güvenlik alanında kapsamlı bir bilgi ve beceri seti ile donatılmakta ve bu alanda kariyer yapmaları için gerekli hazırlığı sağlamaktadır (Daily Sabah, 2023). Üniversitelerin siber güvenlik müfredatları, uluslararası standartlara uygun olarak hazırlanmakta ve sürekli olarak güncellenmektedir (EC-Council, 2024).

Bu eğitim müfredatları, öğrencilerin siber güvenlik alanında derinlemesine bilgi sahibi olmalarını ve pratik beceriler kazanmalarını sağlamaktadır. Ayrıca, üniversiteler, bu alanda ARGE çalışmalarını teşvik etmekte ve öğrencilere bu alanda projeler yapma imkânı sunmaktadır. Bu sayede, öğrenciler pratik ve teorik kazanımlarla donatılmakta ve siber güvenlik alanında kariyer yapmaya hazır hale gelmektedir (Daily Sabah, 2023).

Aşağıda QS 2025 Dünya Sıralamaları'nda ilk 1000'e giren 11 Türk Üniversitesi ve bu üniversitelerin siber güvenlik programları ve de faaliyetleri verilmektedir.

Tablo 3 *QS 2025 Dünya Sıralamalarında İlk 1000'e Giren 11 Türk Üniversitesi (Yükseköğretim Kurulu [YÖK], 2024)*

Ülke Sırası	Üniversite Adı	Dünya Sıralaması
1	**ODTÜ**	**285**
2	**İTÜ**	**326**
3	**Koç Üniversitesi**	**401**
4	**Boğaziçi Üniversitesi**	**418**
5	**Bilkent Üniversitesi**	**477**
6	**Sabancı Üniversitesi**	**516**
7	**İstanbul Üniversitesi**	**621-630**
8	**Hacettepe Üniversitesi**	**641-650**
9	**Ankara Üniversitesi**	**801-850**
10	**Yıldız Teknik Üniversitesi**	**851-900**
11	**Gazi Üniversitesi**	**901-950**

4.4.1.1.Orta Doğu Teknik Üniversitesi (ODTÜ)

ODTÜ Siber Güvenlik Laboratuvarı:

ODTÜ, siber güvenlik alanında araştırmalar yapmakta ve öğrencilere pratik beceriler kazandırmaktadır. ODTÜ'deki siber güvenlik laboratuvarı, öğrencilerin siber saldırılara karşı korunma ve savunma tekniklerini uygulamalı olarak öğrenmelerine imkân tanır (ODTÜ, 2023; Siber Kulüpler Birliği, 2023).

ODTÜ'nün siber güvenlik laboratuvarı, öğrencilere geniş çapta uygulamalı eğitim fırsatları sunmakta ve siber güvenlik alanında çeşitli araştırmalar

yürütmektedir. Laboratuvarda gerçekleştirilen projeler, öğrencilerin siber saldırılara karşı korunma ve savunma tekniklerini uygulamalı olarak öğrenmelerine imkân tanımaktadır. Ayrıca, laboratuvarda gerçekleştirilen araştırmalar, siber güvenlik alanındaki yeni teknolojilerin geliştirilmesine katkı sağlamaktadır (ODTÜ, 2023; Siber Kulüpler Birliği, 2023).

ODTÜ Siber Güvenlik Yüksek Lisans Programı

Orta Doğu Teknik Üniversitesi (ODTÜ) Enformatik Enstitüsü tarafından sunulan Siber Güvenlik Yüksek Lisans Programı, dijital çağda bilgi güvenliğinin kritik önemini kavrayarak, öğrencileri ileri düzey güvenlik uzmanları olarak yetiştirmeyi hedeflemektedir. Program, bilgisayar sistemlerinin güvenliği, siber saldırılara karşı alınması gereken önlemler ve risk yönetimi gibi konulara odaklanır. Öğrencilere, teorik bilgi ile pratik becerileri harmanlayarak, siber güvenlikte uzmanlaşma fırsatı sunulur (Orta Doğu Teknik Üniversitesi, t.y.).

Tablo 4 *ODTÜ Siber Güvenlik Yüksek Lisans Programı Zorunlu Dersler (Orta Doğu Teknik Üniversitesi, t.y.).*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
CSEC 501	Siber Sistemler ve Bilgi Güvenliği	3+0+0	Zorunlu	8
CSEC 502	Ağ Güvenliği	3+0+0	Zorunlu	8

Tablo 5 *ODTÜ Siber Güvenlik Yüksek Lisans Programı Seçmeli Dersler (Orta Doğu Teknik Üniversitesi, t.y.).*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
CSEC 503	Kriptografi	3+0+0	Seçmeli	8
CSEC 504	Zararlı Yazılım Analizi	3+0+0	Seçmeli	8
CSEC 505	Bilgi Güvenliği Yönetimi	3+0+0	Seçmeli	8
CSEC 506	Siber Olaylara Müdahale	3+0+0	Seçmeli	8
CSEC 507	Kurumsal Güvenlik Politikaları	3+0+0	Seçmeli	8
CSEC 508	Bilgi Güvenliği Hukuku	3+0+0	Seçmeli	8

4.4.1.2.İstanbul Teknik Üniversitesi (İTÜ):

Eğitim Programları:

Türkiye'deki İlk Siber Güvenlik Mühendisliği Lisans Programı:

İstanbul Teknik Üniversitesi (İTÜ) Siber Güvenlik Mühendisliği Lisans Programı, 2024-2025 eğitim-öğretim yılında ilk öğrencilerini kabul edecektir. Program, dijital çağın karmaşık zorluklarıyla başa çıkabilen yüksek vasıflı ve etik siber güvenlik profesyonelleri yetiştirmeyi amaçlar. Bu programda teorik bilgi, pratik becerilerle birleştirilir ve öğrencilerin siber güvenlik konusunda bütünsel bir anlayış kazanmaları sağlanır (İTÜ, 2024).

Tablo 6 *(İTÜ) Siber Güvenlik Mühendisliği Lisans Programı Eğitim Programı ve Ders İçerikleri 1. Yarıyıl (İTÜ, 2024).*

Ders	Kredi	Ders
Physics I (FIZ 101E)	3	3
Physics I Lab (FIZ 101EL)	1	0
Introduction to Information Systems (BLG 101E)	2	1
Introduction to Computer Engineering & Ethics (BLG 113E)	1.5	1
Mathematics I (MAT 103E)	4	3
Linear Algebra and Applications (MAT 281E)	3	3
EAP Through Global Goals (ING 100E)	3	3

Tablo 7 *Siber Güvenlik Mühendisliği Lisans Programı Eğitim Programı ve Ders İçerikleri 2. Yarıyıl (İTÜ, 2024).*

Ders	Kredi	Ders
Mathematics II (MAT 104E)	4	3
Discrete Mathematics (BLG 112E)	3	3
Introduction to Scientific and Engineering Computing (C) (BLG 102E)	4	3
Physics II (FIZ 102E)	3	3
Physics II Lab (FIZ 102EL)	1	0
Basics of Academic Writing (ING 112A)	3	3

Tablo 8 *Siber Güvenlik Mühendisliği Lisans Programı Eğitim Programı ve Ders İçerikleri 3. Yarıyıl (İTÜ, 2024).*

Ders	Kredi	Ders
Data Structures (BLG 223E)	3.5	3
Digital Circuits (BLG 231E)	3	3
Engineering Mathematics (BLG 201E)	4	4
Essentials of Research Paper Writing (ING 201A)	3	3
ITB Elective I	3	3
Turkish Language I (TUR 121)	0	2

Tablo 9 *Siber Güvenlik Mühendisliği Lisans Programı Eğitim Programı ve Ders İçerikleri 4. Yarıyıl (İTÜ, 2024).*

Ders	Kredi	Ders
Object Oriented Programming (BLG 252E)	3	3
Formal Languages and Automata (BLG 311E)	3	3
Introduction to Cyber Security (SEC 101E)	3	3
Numerical Methods in Computer Engineering (BLG 202E)	3	3
Computer Organization (BLG 222E)	3	3
ITB Elective II	3	3
Turkish Language II (TUR 122)	0	2

Tablo 10 *Siber Güvenlik Mühendisliği Lisans Programı Eğitim Programı ve Ders İçerikleri 5. Yarıyıl (İTÜ, 2024).*

Ders	Kredi	Ders
Computer Security (BLG 459E)	2	2
Database Systems (BLG 317E)	3	3
Analysis of Algorithms I (BLG 335E)	3	3
Computer Networks (BLG 430E)	2	2
Probability and Statistics (MAT 271E)	3	3
TM Elective I	3	3
Atatürk Principles and Revolution History I (ATA 101)	0	2

Tablo 11 Siber Güvenlik Mühendisliği Lisans Programı Eğitim Programı ve Ders İçerikleri 6. Yarıyıl (İTÜ, 2024).

Ders	Kredi	Ders
Computer Architecture (BLG 322E)	3	2
Analysis of Algorithms II (BLG 336E)	3	3
Atatürk Principles and Revolution History II (ATA 102)	0	2
Computer Operating Systems (BLG 312E)	3	3
Signal and Systems for Communication (BLG 354E)	3	3

Tablo 12 Siber Güvenlik Mühendisliği Lisans Programı Eğitim Programı ve Ders İçerikleri 7. Yarıyıl (İTÜ, 2024).

Ders	Kredi	Ders
Fundamentals of Cryptography (SEC 411E)	3	3
Cyber Security Engineering Design I (SEC 4901E)	3	1
MT Elective I	3	3
MT Elective II	3	3
MT Elective III	3	3

Tablo 13 Siber Güvenlik Mühendisliği Lisans Programı Eğitim Programı ve Ders İçerikleri 8. Yarıyıl (İTÜ, 2024).

Ders	Kredi	Ders
Economics (EKO 201E)	3	3
Cyber Security Engineering Design II (SEC 4902E)	5	1
Secure Programming (BLG 460E)	2	2
MT Elective IV	3	3
MT Elective V	3	3

İstanbul Teknik Üniversitesi (İTÜ) Siber Güvenlik Meslek Yüksekokulu

Siber Güvenlik Meslek Yüksekokulu "Siber Güvenlik Analistliği ve Operatörlüğü" programı 2023-2024 öğretim yılında açılmış olup, öğrencilere ağ güvenliği, zararlı yazılım analizi ve siber tehdit istihbaratı gibi konularda kapsamlı eğitimler sunmaktadır. Programın dili en az %30 İngilizce olup, bir yıl İngilizce hazırlık dahil toplam 3 yıl sürmektedir. (İTÜ Siber Güvenlik Meslek Yüksekokulu, 2023).

İTÜ Siber Güvenlik Meslek Yüksekokulu'nun müfredatı, 6 dönemlik derslerden oluşur. İlk iki dönem temel meslek dersleri, üçüncü ve dördüncü dönemlerde daha ileri seviye meslek dersleri, beşinci ve altıncı dönemlerde ise seçmeli meslek dersleri yer almaktadır. Dersler arasında kriptografi, ağ güvenliği, veri tabanı güvenliği ve siber tehdit analizi gibi konular bulunmaktadır (İTÜ Siber Güvenlik Meslek Yüksekokulu, 2023).

İTÜ'de siber güvenlik alanında faaliyet gösteren çeşitli öğrenci kulüpleri bulunmaktadır. Bu kulüpler, öğrencilerin teorik bilgilerini pratikte uygulayabilecekleri etkinlikler, yarışmalar ve projeler düzenlemektedir. Ayrıca, İTÜ'de düzenlenen "Veri Koruma Günü" ve "Yapay Zekâ Çalıştayı" gibi etkinlikler de öğrencilere sektördeki yenilikleri takip etme imkânı sunmaktadır (İstanbul Teknik Üniversitesi, 2024a; İstanbul Teknik Üniversitesi, 2024b)

4.4.1.3.Koç Üniversitesi:

Koç Üniversitesi, siber güvenlik alanında ileri düzey araştırmalar ve projeler yürütmektedir. Üniversitenin siber güvenlik araştırma merkezi, öğrencilere uygulamalı eğitim fırsatları sunar ve siber tehditlere karşı etkili savunma stratejileri geliştirmelerine yardımcı olur (Kurnaz & Önen, 2019). Koç

Üniversitesi, siber güvenlik alanında çeşitli yüksek lisans programları sunmaktadır (Koç Üniversitesi, 2023).

Koç Üniversitesi'nin siber güvenlik araştırma merkezi, öğrencilere geniş çapta uygulamalı eğitim fırsatları sunmakta ve çeşitli siber güvenlik projeleri üzerinde çalışmaktadır. Bu projeler, öğrencilerin siber tehditleri tanıma, analiz etme ve bu tehditlere karşı savunma stratejileri geliştirme becerilerini artırmaktadır. Ayrıca, merkezde gerçekleştirilen araştırmalar, siber güvenlik alanındaki yeni teknolojilerin geliştirilmesine katkı sağlamaktadır (Koç Üniversitesi, 2023).

Koç Üniversitesi, dünya genelinde artan siber güvenlik ve sistem uzmanı ihtiyacını karşılamak amacıyla, kriptoloji, bilgisayar ağları, işletim sistemleri, yazılım mühendisliği, bulut sistemleri, dağıtık sistemler, yapay zekâ, makine öğrenmesi, risk analizi, stratejik planlama ve ceza hukuku gibi birçok disiplini bir araya getiren yenilikçi bir *Siber Güvenlik Yüksek Lisans Programı* sunmaktadır. Bu program, öğrencilerini alanında uzman ve nitelikli bireyler olarak yetiştirmeyi hedeflemektedir (Koç Üniversitesi, n.d.; Akademik Planlama ve Geliştirme Direktörlüğü).

Koç Üniversitesi, ayrıca siber güvenlik, siber adli bilişim, blokzincir ve kripto paralar, yapay öğrenme, çağdaş kriptoloji (zorunlu ders), uygulamalı sızma testleri, internet ve bulut güvenliği, bulut bilişim güvenliği, bilgisayar sistemleri ve çağdaş uygulamalar güvenliği, siber güvenlik ve veri gizliliği hukuku, bilgisayar ve ağ güvenliği (zorunlu ders), güvenli kod ve yazılım testi, Python ile veri bilimlerine giriş, stratejik sistem modellemesi, dijital dönüşüm, büyük veri ve veri analitiği, bilgisayar ağları, bilişim kuramı, dağıtık bilgisayar sistemleri, paralel programlama, derin öğrenme, algoritma tasarımı ve öğrenmesi, yazılım güvenilirliği, rastgele süreçler, kablosuz haberleşme, kablosuz ağlar, sayılar kuramı, olasılık kuramı, eniyileme modelleri ve algoritmaları, rassal modeller ve uygulamaları, karar analizi, dinamik programlama, buluşsal yöntemler, kuyruk kuramı ve güvenilirlik kuramı gibi dersler sunmaktadır (Koç Üniversitesi, n.d.; Fen Bilimleri ve Mühendislik Enstitüsü).

Tablo 14 *Koç Üniversitesi Siber Güvenlik Yüksek Lisans Programı Dersleri (Koç Üniversitesi, 2024)*

Ders Kodu	Ders Adı	İçerik
CYBR 534	**Computer and Network Security**	Bilgisayar ve ağ güvenliği, ağ protokolleri, güvenlik açıkları, saldırı tespit yöntemleri ve ağ güvenliği stratejileri üzerine odaklanır.
CYBR 543	**Modern Cryptography**	Kriptografi teknikleri, simetrik ve asimetrik şifreleme, dijital imza, anahtar yönetimi ve güvenlik protokolleri gibi modern kriptografi yöntemlerini kapsar.
CYBR 501	**Foundations for Cyber Security**	Siber güvenliğin temelleri, tehdit modelleme, risk yönetimi, güvenlik politikaları ve standartları hakkında genel bilgi verir.
CYBR 503	**Cyber Forensics**	Dijital adli bilişim, delil toplama, analiz ve sunum teknikleri, olay müdahalesi ve yasal prosedürler üzerine odaklanır.
CYBR 509	**Blockchain & Crypto Currencies**	Blockchain teknolojisi, kripto paralar, güvenlik protokolleri ve uygulamaları ele alınır.
CYBR 521	**Introduction to Machine Learning**	Makine öğrenmesine giriş, temel algoritmalar, veri analizi ve uygulamaları içerir.
CYBR 505	**Applied Penetration Testing**	Penetrasyon testi teknikleri, güvenlik açıklarını bulma ve raporlama, uygulamalı saldırı simülasyonları üzerine odaklanır.
CYBR 512	**Internet & Cloud Security**	İnternet ve bulut bilişimde güvenlik, veri koruma, erişim kontrolü ve güvenlik standartları ele alınır.
CYBR 514	**Cloud Computing & Security**	Bulut bilişim altyapısı, güvenlik tehditleri, veri güvenliği ve güvenli bulut mimarisi konularını kapsar.

Tablo 14 *(Devamı-1)*

Ders Kodu	Ders Adı	İçerik
CYBR 545	**Computer Systems & Modern Application Security**	Bilgisayar sistemleri güvenliği, modern uygulama güvenliği, saldırı tespit ve önleme teknikleri üzerinde durulur.
CYBR 571	**Cyber Security & Data Protection Law**	Veri koruma kanunları, KVKK ve GDPR, siber hukuk ve düzenlemeler hakkında bilgi verir.
CYBR 507	**Secure Software Coding and Testing**	Güvenli yazılım geliştirme, kodlama standartları ve güvenlik testi yöntemlerini içerir.
DASC 501	**Introduction to Data Science with Python**	Python kullanarak veri bilimine giriş, veri analizi, modelleme ve veri işleme tekniklerini kapsar.
TECH 517	**Strategic Systems Modeling**	Stratejik sistem modelleme, sistem dinamikleri ve karar verme süreçlerini kapsar.
TECH 570	**Digital Transformation**	Dijital dönüşüm süreçleri, stratejileri ve teknolojileri üzerine odaklanır.
TECH 512	**Big Data & Data Analytics**	Büyük veri analitiği, veri işleme teknikleri ve büyük veri teknolojileri içerir.
COMP 416	**Computer Networks**	Bilgisayar ağları, ağ mimarisi, yönlendirme protokolleri ve ağ güvenliği üzerine odaklanır.
COMP 513	**Information Theory**	Bilgi teorisi, kodlama teorisi ve iletişim sistemleri üzerinde durulur.
COMP 515	**Distributed Computing Systems**	Dağıtık sistemler, paralel hesaplama ve dağıtık veri işleme tekniklerini kapsar.

Tablo 14 *(Devamı-2)*

Ders Kodu	Ders Adı	İçerik
COMP 521	**Introduction to Machine Learning**	Makine öğrenmesine giriş, temel algoritmalar, veri analizi ve uygulamaları içerir.
COMP 529	**Parallel Programming**	Paralel programlama, çok çekirdekli sistemlerde programlama ve paralel algoritmalar üzerine odaklanır.
COMP 541	**Deep Learning**	Derin öğrenme teknikleri, sinir ağları ve derin öğrenme uygulamaları içerir.
COMP 546	**Algorithm Design and Analysis**	Algoritma tasarımı, analiz teknikleri ve karmaşıklık teorisi üzerinde durulur.
COMP 589	**Software Reliability: Specification, Testing, and Verification**	Yazılım güvenilirliği, yazılım testi, doğrulama ve yazılım güvenlik standartları ele alınır.
ELEC 501	**Random Processes**	Rastgele süreçler, olasılık teorisi ve stokastik modelleme üzerine odaklanır.
ELEC 514	**Wireless Communications**	Kablosuz iletişim sistemleri, frekans tahsisi, sinyal işleme ve kablosuz ağ güvenliği içerir.
ELEC 528	**Wireless Networks**	Kablosuz ağlar, ağ protokolleri, mobil iletişim ve kablosuz ağ güvenliği üzerine odaklanır.
MATH 527	**Number Theory**	Sayı teorisi, asal sayılar, modüler aritmetik ve kriptografik uygulamaları içerir.
MATH 541	**Probability Theory**	Olasılık teorisi, stokastik süreçler ve rastgele değişkenler üzerinde durulur.

Tablo 14 *(Devamı-3)*

Ders Kodu	Ders Adı	İçerik
INDR 501	**Optimization Models and Algorithms**	Optimizasyon modelleri, algoritmalar ve matematiksel programlama tekniklerini kapsar.
INDR 503	**Stochastic Models and Their Applications**	Stokastik modeller, uygulamaları ve rastgele süreçlerin analizi üzerinde durulur.
INDR 530	**Decision Analysis**	Karar analizi, risk değerlendirmesi ve karar verme teorileri içerir.
INDR 564	**Dynamic Programming**	Dinamik programlama, optimizasyon teknikleri ve karar verme süreçlerini kapsar.
INDR 568	**Heuristic Methods**	Sezgisel yöntemler, optimizasyon problemlerinin çözümü için kullanılan algoritmalar üzerine odaklanır.
INDR 570	**Queueing Theory**	Kuyruk teorisi, servis sistemleri ve performans analizi üzerinde durulur.
INDR 572	**Reliability Theory**	Güvenilirlik teorisi, sistem güvenilirliği analizi ve arıza modellemesi içerir.

4.4.1.4.Boğaziçi Üniversitesi:

Boğaziçi Üniversitesi 1 Aralık 2016 tarihinde siber güvenliğin gerektirdiği uzmanlık ve odaklanmayı sağlamak amaçlı BÜSİBER (Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi) 'i kurmuş ve akademik bakış açısıyla siber güvenlik ve kişisel verilerin korunması konularında farkındalık oluşturarak ülkemizde bu alanda ihtiyaç duyulan yetişmiş insan kaynağı açığını kapatmaya destek vermeyi hedeflemiştir (Boğaziçi Üniversitesi Siber Güvenlik Merkezi, t.y.).

Siber Güvenlik Eğitimi ve Programları

Boğaziçi Üniversitesi, Türkiye'de siber güvenlik eğitimi konusunda önemli bir merkezdir. Üniversite bünyesinde faaliyet gösteren BÜSİBER (Boğaziçi Üniversitesi Siber Güvenlik Merkezi), öğrencilere yönelik ücretsiz yaz ve kış siber kampları düzenlemektedir. Bu kamplar, siber güvenlik farkındalığını artırmak ve öğrencilere uygulamalı eğitimler sunmak amacıyla gerçekleştirilir. (Boğaziçi Üniversitesi, 2023).

Programın İçeriği:

Temel Bilgi Güvenliği ve Mahremiyet: Bilgi güvenliğinin temel ilkeleri ve uygulamaları.

Siber Tehditler ve Korunma Yöntemleri: Güncel siber tehditler ve bu tehditlere karşı alınabilecek önlemler.

Veri Güvenliği ve Yönetimi: Verilerin güvenli bir şekilde yönetimi ve korunması.

Adli Bilişim: Adli bilişim teknikleri ve teknolojileri.

Beyaz Şapkalı Etik Hacker Eğitimi: Ethical hacking, ağ tarama ve güvenlik açığı analizi.

Siber Olaylara Müdahale Eğitimi: Olay müdahale süreçleri ve teknik analiz yöntemleri.

Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi (BÜSİBER) ‘nin yanı sıra, KoçSistem iş birliğiyle iş garantili siber güvenlik eğitim programları da sunulmaktadır. Bu programlar, öğrencilerin kariyerlerini siber güvenlik alanında sürdürmelerine olanak tanımaktadır.

4.4.1.5.Bilkent Üniversitesi:

İhsan Doğramacı Bilkent Üniversitesi Siber Güvenlik Programı

İhsan Doğramacı Bilkent Üniversitesi, siber güvenlik alanında öğrencilere geniş kapsamlı eğitim ve araştırma imkânları sunmaktadır (Bilkent University, 2023).

Bilkent Üniversitesi, Bilgisayar Mühendisliği Bölümü bünyesinde siber güvenlik konularında çeşitli dersler sunmaktadır. Bu dersler arasında ağ güvenliği, kriptografi, zararlı yazılım analizi ve güvenli yazılım geliştirme gibi konular yer almaktadır. Ayrıca, öğrenciler pratik uygulamalar ve projelerle bu alanda deneyim kazanma fırsatına sahiptir.

Üniversite, siber güvenlik alanında önemli araştırma projelerine ev sahipliği yapmaktadır. Bilkent Üniversitesi'nin araştırma merkezleri, siber güvenlik konularında ileri düzey araştırmalar yürütmekte ve bu alanda öğrencilere önemli katkılar sağlamaktadır. Öğrenciler, akademisyenlerle birlikte çeşitli projelerde yer alarak pratik deneyim kazanmaktadır (Bilkent University, 2023).

4.4.1.6.Sabancı Üniversitesi:

Sabancı Üniversitesi Siber Güvenlik Programı

Eğitim Programları:

Sabancı Üniversitesi, siber güvenlik alanında lisansüstü düzeyde kapsamlı eğitim programları sunmaktadır. Üniversitenin Mühendislik ve Doğa Bilimleri Fakültesi bünyesinde yer alan Siber Güvenlik Yüksek Lisans ve Doktora Programları, öğrencilere ağ güvenliği, kriptografi, zararlı yazılım analizi, adli bilişim ve blockchain teknolojileri gibi konularda ileri düzey eğitimler sunmaktadır (Sabancı Üniversitesi, 2023).

Siber güvenlik programının müfredatında kriptografi, ağ güvenliği, zararlı yazılım analizi, adli bilişim ve blockchain güvenliği gibi dersler yer almaktadır. Öğrenciler ayrıca veri güvenliği, mahremiyet, yazılım güvenliği ve biyometrik sistemler gibi konularda da eğitim almaktadırlar. Bu dersler, öğrencilere güncel siber güvenlik problemlerine yönelik kapsamlı bir eğitim sunmayı amaçlamaktadır (Sabancı Üniversitesi, 2023).

Sabancı Üniversitesi'nde aktif bir Siber Güvenlik Kulübü bulunmaktadır. Bu kulüp, öğrencilere siber güvenlik seminerleri, hackathonlar ve proje yarışmaları gibi etkinlikler düzenleyerek teorik bilgilerini pratiğe dönüştürme fırsatı sunmaktadır. Kulüp, aynı zamanda sektördeki uzmanlarla düzenlenen etkinliklerle öğrencilerin kariyer gelişimlerine destek olmaktadır (Sabancı Üniversitesi, 2023).

4.4.1.7.İstanbul Üniversitesi:

İstanbul Üniversitesi Siber Güvenlik Programı

Eğitim Programları:

İstanbul Üniversitesi, siber güvenlik alanında kapsamlı eğitim programları sunmaktadır. Üniversitenin Fen Fakültesi, çeşitli lisans ve lisansüstü programlar kapsamında siber güvenlik eğitimi vermektedir. Bu programlar, ağ güvenliği, zararlı yazılım analizi, kriptografi ve siber tehdit istihbaratı gibi konularda derinlemesine bilgi sağlamaktadır. Özellikle Fen Fakültesi bünyesindeki siber güvenlik dersleri, teorik bilgilerin yanı sıra pratik uygulamalarla desteklenmektedir (İstanbul Üniversitesi, 2023).

Program kapsamında verilen dersler arasında ağ güvenliği, zararlı yazılım analizi, kriptografi ve veri koruma yer almaktadır. Öğrenciler, bu dersler aracılığıyla hem teorik bilgi edinmekte hem de laboratuvar çalışmaları ve projelerle pratik beceriler kazanmaktadır. Müfredat, siber güvenlik alanında güncel ve gerekli tüm konuları kapsamaktadır (İstanbul Üniversitesi, 2023).

İstanbul Üniversitesi'nde siber güvenlik alanında faaliyet gösteren çeşitli öğrenci kulüpleri bulunmaktadır. Bu kulüpler, öğrencilerin teorik bilgilerini uygulamaya dönüştürebilecekleri etkinlikler, seminerler ve yarışmalar düzenlemektedir. Ayrıca, Türkiye Siber Güvenlik Kümelenmesi tarafından düzenlenen Siber Güvenlik Yaz Kampı gibi etkinliklere de katılım imkanı sunulmaktadır. Bu kamplar, öğrencilere geniş kapsamlı eğitimler ve pratik deneyimler kazandırmaktadır.

Etkinlikler:

İstanbul Üniversitesi, siber güvenlik alanında çeşitli etkinlikler düzenlemektedir. Örneğin, Siber Güvenlik Haftası etkinlikleri kapsamında, siber güvenlik uzmanlarının katıldığı paneller ve atölye çalışmaları düzenlenmektedir. Bu etkinlikler, öğrencilerin sektördeki yenilikleri ve gelişmeleri takip etmelerine olanak tanımaktadır.

4.4.1.8.Hacettepe Üniversitesi:

Hacettepe Üniversitesi, bilgi güvenliği ve kriptografi konularında araştırmalar yapmakta ve öğrencilere eğitimler sunmaktadır. Bu merkezde gerçekleştirilen

projeler, öğrencilere veri güvenliği, şifreleme teknikleri ve siber tehditlere karşı korunma stratejileri konularında bilgi ve beceriler kazandırmaktadır.

Hacettepe Üniversitesi'nin bilgi güvenliği ve kriptografi araştırma merkezi, öğrencilere geniş çapta teorik bilgi ve pratik beceriler kazandırmayı hedeflemektedir. Merkezde gerçekleştirilen projeler, veri güvenliği, şifreleme teknikleri ve siber tehditlere karşı korunma stratejileri konularında öğrencilere bilgi ve beceriler kazandırmaktadır. Ayrıca, merkezde gerçekleştirilen araştırmalar, bilgi güvenliği ve kriptografi alanındaki yeni teknolojilerin geliştirilmesine katkı sağlamaktadır.

4.4.1.9.Ankara Üniversitesi:

Siber Güvenlik Eğitimi ve Programları

Ankara Üniversitesi, siber güvenlik eğitimi konusunda çeşitli programlar sunmaktadır. Üniversite bünyesinde 2023 yılında kurulan Siber Güvenlik Meslek Yüksekokulu, siber güvenlik alanında nitelikli uzmanlar yetiştirmeyi hedeflemektedir (Ankara Üniversitesi, 2023).

Programın İçeriği:

- **Siber Güvenlik Analistliği ve Operatörlüğü**: Program kapsamında Siber Güvenlik Olay Analisti, SGOM/SOME 1. Seviye Destek Elemanı, Siber Tehdit İstihbarat Analisti ve Siber Güvenlik Sistemleri Operatörü yetiştirilmektedir.
- **Temel Bilgi Güvenliği:** Bilgi güvenliğinin temel ilkeleri ve uygulamaları.
- **Bilgisayar Olay Analizi ve Müdahale Teknikleri:** Siber olaylara müdahale yöntemleri ve teknik analiz süreçleri.
- **Güvenli Yazılım Geliştirme:** Güvenli yazılım geliştirme süreçleri ve yazılım güvenliği.
- **Siber Güvenlik Operasyon Yönetimi:** Siber güvenlik operasyon merkezleri ve yönetim süreçleri.

Adli Bilişim: Adli Bilişim Teknikleri Ve Teknolojileri

Program üç yıl sürmekte olup, bir yıl İngilizce hazırlık ve toplam altı dönemlik bir eğitim sunulmaktadır. Öğrencilere teorik ve uygulamalı derslerin yanı sıra teknoparklarda staj imkânı da sağlanmaktadır. Programın %30'u İngilizce olarak yürütülmektedir (Ankara Üniversitesi, 2023).

4.4.1.10. Yıldız Teknik Üniversitesi:

Yıldız Teknik Üniversitesi Siber Güvenlik Programı

Yıldız Teknik Üniversitesi, siber güvenlik alanında kapsamlı eğitim programları sunmaktadır. Üniversitenin Bilgisayar Mühendisliği Bölümü, öğrencilere ağ güvenliği, zararlı yazılım analizi, kriptografi ve siber tehdit istihbaratı gibi konularda geniş bir bilgi birikimi sağlar (Yıldız Teknik Üniversitesi, 2023a).

Siber güvenlik programının müfredatında zorunlu ve seçmeli dersler bulunmaktadır. Temel dersler arasında kriptografi, ağ güvenliği, zararlı yazılım analizi, adli bilişim ve siber tehdit istihbaratı yer almaktadır. Ayrıca, blockchain teknolojisi ve veri güvenliği gibi ileri düzey dersler de bulunmaktadır. Bu dersler, öğrencilere siber güvenlik alanında kapsamlı ve güncel bir eğitim sunmayı amaçlamaktadır (Yıldız Teknik Üniversitesi, 2023a).

Yıldız Teknik Üniversitesi (YTU) bünyesinde, siber güvenlik alanında çeşitli yüksek lisans programları bulunmaktadır. Bu programlar, öğrencilere siber güvenlik, kriptografi, ağ güvenliği gibi kritik konularda kapsamlı bir eğitim sunmaktadır. Fen Bilimleri Enstitüsü tarafından sunulan bu programlar hem tezli hem de tezsiz seçenekler ile öğrencilere akademik ve profesyonel kariyerlerinde derinlemesine bilgi ve beceriler kazandırmayı amaçlamaktadır (Yıldız Teknik Üniversitesi, 2023b).

Siber Güvenlik ile İlgili Dersler ve Programlar (Yıldız Teknik Üniversitesi, 2023b).

Aşağıda, YTÜ'nün Siber Güvenlik ve Kriptografi alanındaki yüksek lisans programlarında sunulan derslerin detayları tablo halinde verilmiştir:

Tablo 15 *YTÜ Siber Güvenlik ve Kriptografi Alanındaki Yüksek Lisans Programlarında Sunulan Dersler (Yıldız Teknik Üniversitesi, 2023b).*

Ders Kodu	Ders Adı	Kredi	AKTS
CS7001	Ağ Güvenliği (Network Security)	3	6
CS7002	Kriptografi (Cryptography)	3	6
CS7003	Bilgi Güvenliği Yönetimi (Information Security Management)	3	6
CS7004	Siber Güvenlik Tehditleri ve Savunma (Cybersecurity Threats and Defense)	3	6
CS7005	Güvenlik Protokolleri (Security Protocols)	3	6
CS7006	Güvenli Yazılım Geliştirme (Secure Software Development)	3	6
CS7007	Etik Hacking (Ethical Hacking)	3	6

Yıldız Teknik Üniversitesi'nde siber güvenlik ile ilgili aktif öğrenci kulüpleri bulunmaktadır. Bu kulüpler, siber güvenlik seminerleri, hackathonlar ve proje yarışmaları gibi etkinlikler düzenleyerek öğrencilere teorik bilgilerini pratiğe dönüştürme fırsatı sunmaktadır (Türkiye Bilişim Derneği, 2023).

4.4.1.11. Gazi Üniversitesi:

Gazi Üniversitesi Siber Güvenlik Eğitimi ve Programları

Programlar ve Dersler: Gazi Üniversitesi, siber güvenlik alanında kapsamlı eğitim programları sunmaktadır. Bilgisayar Mühendisliği Bölümü bünyesinde, öğrenciler ağ güvenliği, kriptografi, zararlı yazılım analizi ve güvenli yazılım geliştirme gibi konularda çeşitli dersler alabilirler. Bu dersler, teorik bilgilerin yanı sıra pratik uygulamalarla desteklenir ve öğrencilere alanda yetkinlik kazandırmayı amaçlar (Gazi Üniversitesi, 2023).

Bilgi Güvenliği Yükseklisans ve Doktora Programı

Gazi Üniversitesi Fen Bilimleri Enstitüsü bünyesinde sunulan Bilgi Güvenliği Mühendisliği programı, artan siber saldırı tehditleri ve karmaşıklıklarıyla başa çıkmayı hedeflemektedir. Bilgi güvenliğinin ulusal güvenliğin ayrılmaz bir parçası olarak kabul edilmesiyle, program, Siber Güvenlik, Ağ Güvenliği, İnternet Güvenliği ve Uygulama Güvenliği gibi çeşitli alanlar arasındaki boşlukları kapatmayı amaçlamaktadır. Programın temel amacı, karmaşık güvenlik sorunlarını çözebilecek nitelikli Bilgi Güvenliği Mühendisleri yetiştirmektir ve ulusal ve uluslararası siber güvenlik ekosistemine katkıda bulunmaktır (Gazi Üniversitesi Fen Bilimleri Enstitüsü, t.y.).

Misyon: Bilgi Güvenliği Mühendisliği programının misyonu, öğrencilerine gerekli bilgi, beceri ve yetkinlikleri kazandırarak, siber güvenlik sektörünün ihtiyaçlarını karşılamaktır. Program, teknolojik gelişmeleri takip ederek ülkenin siber güvenlik ekosistemine ve ekonomisine önemli katkılar sağlamayı amaçlamaktadır (Gazi Üniversitesi Fen Bilimleri Enstitüsü, t.y.).

Vizyon: Programın vizyonu, ulusal ve uluslararası düzeyde bilgi güvenliği alanında tanınan ve yetkin Bilgi Güvenliği Uzmanları yetiştiren önde gelen programlar arasında yer almaktır(Gazi Üniversitesi Fen Bilimleri Enstitüsü, t.y.).

Programın Amaçları (Gazi Üniversitesi Fen Bilimleri Enstitüsü, t.y.).

1. Karmaşık güvenlik sorunlarına çözüm getirebilecek yüksek düzeyde Bilgi Güvenliği Mühendisleri yetiştirmek.
2. Üniversitelerin ihtiyaç duyduğu akademik personeli yetiştirmek ve akademisyen açığını kapatmak.
3. Ülkemizin Bilgi Güvenliği Mühendisliği eğitim ve araştırma kalitesini artırmak.
4. Yüksek katma değerli projelerin üretimini teşvik etmek ve son yıllarda daha fazla fon sağlanan AB Güvenlik projelerinden daha fazla yararlanmak.
5. Ülkemizde bilişim sektörünün güvenli gelişimine katkıda bulunmak.

6. Bilgi Güvenliği sektörünün gelişimine katkıda bulunmak.
7. Ülkemizde düzenlenen ulusal ve uluslararası konferans, sempozyum ve çalıştay sayısını artırmak.
8. İlgili birimlerle iş birliği içinde ulusal çözümler geliştirmek.
9. Uluslararası üniversitelerle iş birliği yaparak uluslararası iş birliğinin gelişmesini sağlamak.
10. Ülkemizin bilimsel prestijini artırmak.
11. Birimlerin/kurumların karşılaştıkları sorunları yerinde çözmek.
12. Hem nitelik hem de nicelik açısından önemli yayınlar üreterek bilim dünyasına katkıda bulunmak ve üniversitemizin ve ülkemizin bilimsel itibarına katkıda bulunmak.

Program, Bilgi Güvenliği'nin çeşitli yönlerine odaklanan hem Yüksek Lisans hem de Doktora dereceleri sunmaktadır. Müfredat, öğrencileri akademi, sanayi ve devlet sektörlerinde ileri düzey rollere hazırlamak için temel dersler, özel seçimlik dersler ve araştırma fırsatlarını içermektedir (Gazi Üniversitesi Fen Bilimleri Enstitüsü, t.y.).

Tablo 16 *Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Dersleri 1. Yarıyıl Ders Planı (Gazi Üniversitesi, t.y.a)*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
BGM5141	Şifrelendirme Metotları	3+0+0	Zorunlu	8
BGM5211	Siber Güvenliğin Temelleri	3+0+0	Zorunlu	8
BGM5241	Büyük Veri ve Kişisel Veri Güvenliği	3+0+0	Zorunlu	8
83FBE5001	Yüksek Lisans Tezine Hazırlık	3+1+0	Zorunlu	5
83FBE5002	Yüksek Lisans Tez Çalışması	3+1+0	Zorunlu	30
83FBE5003	Yüksek Lisans Seminer	0+2+0	Zorunlu	5

Tablo 16 *(Devamı-1)*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
83FBE7001	Bilimsel Araştırma Yöntemleri ve Etik	3+0+0	Zorunlu	6
BGM5111	Yeni Nesil Ağ Güvenliği	3+0+0	Seçmeli	8
BGM5121	Mobil Teknolojilerde Bilgi Güvenliği Riskleri ve Yönetimi	3+0+0	Seçmeli	8
BGM5131	Gömülü Sistem Güvenliği	3+0+0	Seçmeli	8
BGM5151	Saldırı Tespitinde Veri Madenciliği Uygulamaları	3+0+0	Seçmeli	8
BGM5161	Tıbbi Veri Güvenliği ve Steganografi Uygulamaları	3+0+0	Seçmeli	8
BGM5171	Bilgi Güvenliği ve Yönetimi	3+0+0	Seçmeli	8
BGM5181	Kablosuz Sensör Ağlarda Güvenlik	3+0+0	Seçmeli	8
BGM5191	Bilişim Suçları ve Adli Bilişim	3+0+0	Seçmeli	8
BGM5201	Bilgi Teknolojileri Denetimi	3+0+0	Seçmeli	8
BGM5221	Adli Bilişim Hukuku	3+0+0	Seçmeli	8
BGM5231	Mobil Kötücül Yazılım Analizi	3+0+0	Seçmeli	8
BGM5251	Bulut Bilişim Güvenliği	3+0+0	Seçmeli	8
BGM5261	Jeopolitik Gelişmeler, Hibrit Savaş ve Siber Terör	3+0+0	Seçmeli	8
BGM5271	Kişisel ve Kurumsal Verilerin Korunmasında Teknik ve Hukuki Düzenlemeler	3+0+0	Seçmeli	8
BGM5281	Blokzincir Güvenliği ve Dijital Paralar	3+0+0	Seçmeli	8

Tablo 16 *(Devamı-2)*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
BGM5291	Etik Hackleme ve Sızma Testleri	3+0+0	Seçmeli	8
BGM5301	Web Güvenliği	3+0+0	Seçmeli	8
BGM5311	Siber Güvenlikte Derin Öğrenme Teknikleri ve Uygulamaları	3+0+0	Seçmeli	8
BGM5321	Enformasyon Savaşları ve Derin Sahtecilik Uygulamaları	3+0+0	Seçmeli	8
BGM5331	Haberleşme Sinyal İstihbaratı ve Güvenliği	3+0+0	Seçmeli	8
BGM5341	Veri Merkezi Güvenliği	3+0+0	Seçmeli	8
BGM5351	Siber Güvenlikte Açık Kaynak İstihbaratı	0+0+0	Seçmeli	8

Tablo 17 *Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Dersleri 2. Yarıyıl Ders Planı (Gazi Üniversitesi, t.y.a)*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
BGM5021	Siber Savaş, Savunma ve Güvenlik	3+0+0	Zorunlu	9
BGM5011	Bilgi Güv. Müh. Makina Öğrenmesi ve Uyg.	3+0+0	Seçmeli	8
BGM5031	Akıllı Şebekelerde Siber Güvenlik	3+0+0	Seçmeli	8
BGM5041	Ulusal ve Uluslararası Bilgi Güv. Politikaları	3+0+0	Seçmeli	9
BGM5051	Ağlarda Adli Bilişim	3+0+0	Seçmeli	8

Tablo 17 *(Devamı)*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
BGM5061	Sayısal Görüntü ve Video İşlemede Bilgi Güv. Uyg.	3+0+0	Seçmeli	8
BGM5071	Kablosuz Cihaz Güvenliği	3+0+0	Seçmeli	8
BGM5081	Biyometrik Kimlik Doğrulama Sistemleri	3+0+0	Seçmeli	8
BGM5091	Kritik Altyapılar ve Güvenliği	3+0+0	Seçmeli	8
BGM5101	Bilgi Güvenliği Hukuku	3+0+0	Seçmeli	8

Tablo 18 *Bilgi Güvenliği Mühendisliği Doktora Programı Dersleri (Gazi Üniversitesi, t.y.b)*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
BGM5111	Yeni Nesil Ağ Güvenliği	3+0+0	Zorunlu	8
BGM5171	Bilgi Güvenliği ve Yönetimi	3+0+0	Zorunlu	8
83FBE6001	Doktora Tezine Hazırlık	3+1+0	Zorunlu	5
83FBE6002	Doktora Tez Çalışması	3+1+0	Zorunlu	30
83FBE6003	Doktora Seminer	0+2+0	Zorunlu	5
83FBE6004	Yeterlik Sınavı	3+1+0	Zorunlu	25

Tablo 18 *(Devamı-1)*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
83FBE7001	Bilimsel Araştırma Yöntemleri ve Etik	3+0+0	Zorunlu	6
BGM5121	Mobil Teknolojilerde Bilgi Güvenliği Riskleri ve Y	3+0+0	Seçmeli	8
BGM5131	Gömülü Sistem Güvenliği	3+0+0	Seçmeli	8
BGM5141	Şifrelendirme Metotları	3+0+0	Seçmeli	8
BGM5151	Saldırı Tespitinde Veri Madenciliği Uygulamaları	3+0+0	Seçmeli	8
BGM5161	Tıbbi Veri Güvenliği ve Steganografi Uygulamaları	3+0+0	Seçmeli	8
BGM5181	Kablosuz Sensör Ağlarda Güvenlik	3+0+0	Seçmeli	8
BGM5191	Bilişim Suçları ve Adli Bilişim	3+0+0	Seçmeli	8
BGM5201	Bilgi Teknolojileri Denetimi	3+0+0	Seçmeli	8
BGM5221	Adli Bilişim Hukuku	3+0+0	Seçmeli	8
BGM5231	Mobil Kötücü Yazılım Analizi	3+0+0	Seçmeli	8
BGM5241	Büyük Veri ve Kişisel Veri Güvenliği	3+0+0	Seçmeli	8
BGM5251	Bulut Bilişim Güvenliği	3+0+0	Seçmeli	8
BGM5261	Jeopolitik Gelişmeler, Hibrit Savaş ve Siber Terör	3+0+0	Seçmeli	8

Tablo 18 *(Devamı-2)*

Ders Kodu	Ders Adı	T+U+L	Zorunlu/Seçmeli	AKTS
BGM5271	Kişisel ve Kurumsal Verilerin Korunmasında Teknik ve Hukuki Düzenlemeler	3+0+0	Seçmeli	8
BGM5281	Blokzincir Güvenliği ve Dijital Paralar	3+0+0	Seçmeli	8
BGM5291	Etik Hackleme ve Sızma Testleri	3+0+0	Seçmeli	8
BGM5301	Web Güvenliği	3+0+0	Seçmeli	8
BGM5311	Siber Güvenlikte Derin Öğrenme Teknikleri ve Uygulamaları	3+0+0	Seçmeli	8
BGM5321	Enformasyon Savaşları ve Derin Sahtecilik Uygulamaları	3+0+0	Seçmeli	8
BGM5331	Haberleşme Sinyal İstihbaratı ve Güvenliği	3+0+0	Seçmeli	8
BGM5341	Veri Merkezi Güvenliği	3+0+0	Seçmeli	8
BGM5351	Siber Güvenlikte Açık Kaynak İstihbaratı	0+0+0	Seçmeli	8
BGM6171	Bilgi Güvenliği ve Yönetimi	3+0+0	Seçmeli	8
BGM5041	Ulusal ve Uluslararası Bilgi Güvenliği Politikaları	3+0+0	Zorunlu	9
BGM5091	Kritik Altyapılar ve Güvenliği	3+0+0	Zorunlu	8
BGM5011	Bilgi Güvenliği Mühendisliğinde Makina Öğrenmesi ve Uygulamaları	3+0+0	Seçmeli	8
BGM5021	Siber Savaş, Savunma ve Güvenlik	3+0+0	Seçmeli	9
BGM5031	Akıllı Şebekelerde Siber Güvenlik	3+0+0	Seçmeli	8

Tablo 18 (Devamı-3)

BGM5051	**Bilgisayar Ağlarında Adli Analiz**	**3+0+0**	**Seçmeli**	**8**
BGM5061	Sayısal Görüntü ve Video İşlemede Bilgi Güvenliği Uygulamaları	3+0+0	Seçmeli	8
BGM5071	Mobil Cihaz Güvenliği	3+0+0	Seçmeli	8
BGM5081	Biyometrik Kimlik Doğrulama Sistemleri	3+0+0	Seçmeli	8
BGM5101	Bilgi Güvenliği Hukuku	3+0+0	Seçmeli	8

Üniversitede aktif olarak faaliyet gösteren Siber Güvenlik Araştırma ve Geliştirme Topluluğu, öğrencilere bilgi güvenliği ve siber güvenlik konularında eğitimler vererek sektöre yeni yetenekler kazandırmayı hedefler. Ayrıca, Gazi Üniversitesi Mühendislik Fakültesi tarafından düzenlenen TechAnkara Siber Güvenlik Yaz Kampı, öğrencilere siber güvenlik alanında derinlemesine bilgi ve pratik deneyim sağlar. Bu kamp, BTK Akademi ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) iş birliği ile düzenlenmekte ve çeşitli etkinliklerle zenginleştirilmektedir (Gazi Üniversitesi, 2023).

Gazi Üniversitesi Eğitim Fakültesi tarafından düzenlenen "Güvenli ve Bilinçli İnternet Kullanımı Siber Güvenlik Önlemleri" adlı etkinlik, öğrencilere güvenli internet kullanımı konusunda bilinçlendirme sağlamaktadır. Bu etkinlikler, siber güvenlik farkındalığını artırmak amacıyla düzenlenir ve öğrencilere pratik bilgiler sunar (Gazi Üniversitesi, 2023).

4.4.1.12. İstanbul Üniversitesi Cerrahpaşa

İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Bölümü, 2016 yılında yeniden yapılanarak dört ana bilim dalı halinde organize edilmiştir: *Bilgisayar Bilimleri*, *Bilgisayar Donanımı ve Gömülü Sistemler*, *Yazılım Mühendisliği* ve *Siber Güvenlik*. Bu yapılanma, bölüme hem akademik hem de endüstriyel alanlarda daha odaklanmış ve uzmanlaşmış bir eğitim ve araştırma altyapısı sağlamayı amaçlamaktadır (İstanbul Üniversitesi-Cerrahpaşa, 2023d).

İstanbul Üniversitesi-Cerrahpaşa Bilgisayar Mühendisliği Bölümü, siber güvenlik konusunda çeşitli dersler sunmaktadır. Bu dersler, öğrencilerin siber güvenliğin temel prensiplerini öğrenmelerini ve bu alandaki en son teknikleri

uygulamalı olarak öğrenmelerini sağlamaktadır. (İstanbul Üniversitesi-Cerrahpaşa, 2023e).

Tablo 19 *İstanbul Üniversitesi Cerrahpaşa Lisans Programı Bünyesinde Siber Güvenlik Alanında Verilen Dersler (Bilgisayar Mühendisliği / Bilgisayar Bilimleri) (İstanbul Üniversitesi-Cerrahpaşa, 2023e).*

Kriptografi Temelleri	**Şifreleme algoritmaları, anahtar yönetimi, simetrik ve asimetrik şifreleme.**	**4. Yıl / Güz**
Etik Hacking	Sistem güvenliği testi, zafiyet tarama ve penetrasyon testleri.	4. Yıl / Bahar
Bilgisayar Ağları	Bilgisayar ağlarının yapısı, TCP/IP protokolleri, routing ve switching.	2. Yıl / Bahar
Ders Adı	İçerik	Yıl / Dönem
Bilgi Güvenliği	Bilgi güvenliği temel prensipleri, şifreleme teknikleri ve güvenlik protokolleri.	3. Yıl / Güz
Ağ Güvenliği	Ağlar üzerinde güvenlik tehditleri, güvenlik duvarları, VPN ve IDS/IPS sistemleri.	3. Yıl / Bahar

Lisansüstü Programı (Siber Güvenlik Yüksek Lisans)

İstanbul Üniversitesi-Cerrahpaşa, 2023-2024 akademik yılında siber güvenlik alanında tezli yüksek lisans programı sunmaktadır. Bu program, Türkçe dilinde örgün eğitim olarak yürütülmektedir ve 30 kişilik kontenjana sahiptir. Kabul koşulları, ALES puanı, yabancı dil notu ve lisans not ortalaması gibi kriterlere dayanmaktadır. Bilgisayar Mühendisliği ve ilgili bölümlerden mezun olan öğrenciler bilimsel hazırlık programına tabi olmadan kabul edilmektedir. Programın misyonu, ulusal güvenliğin sağlanmasında siber güvenlik uzmanları yetiştirmektir (İstanbul Üniversitesi-Cerrahpaşa, 2023a).

İstanbul Üniversitesi-Cerrahpaşa Siber Güvenlik Yüksek Lisans Programı'nın eğitim amaçları şunlardır:

- Öğrencilerin siber güvenlik alanında temel teorik bilgi ve teknik altyapı edinmeleri,
- Mevcut ve gelecekteki siber saldırıların tespit ve analizi konusunda bilgi sahibi olmaları,
- Siber saldırılara yönelik risk analizi yaparak stratejiler geliştirebilmeleri,
- Güncel teknolojileri ve yazılım araçlarını etkin kullanabilmeleri (İstanbul Üniversitesi-Cerrahpaşa, 2023b).

Tablo 20 *İstanbul Üniversitesi Cerrahpaşa Siber Güvenlik Yüksek Lisans 1. Sınıf - Güz Dönemi Dersleri (İstanbul Üniversitesi-Cerrahpaşa, 2023b).*

Kod	Ders Adı	Kredi	AKTS	Z/S	T/U/L
SBRG7001	AĞ GÜVENLİĞİ	3	6	S	3/0/0
SBRG7006	BİLGİ GÜVENLİĞİ MİMARİLERİ	3	6	S	3/0/0
SBRG7004	BİLGİ GÜVENLİĞİ RİSK YÖNETİMİ	3	6	S	3/0/0
SBRG7010	BİLİMSEL ARAŞTIRMA YÖNTEMLERİ VE YAYIN ETİĞİ	3	8	Z	3/0/0
SBRG7003	BÜYÜK VERİ VE GÜVENLİK	3	6	S	3/0/0
SBRG7008	GRAF TEORİ	3	6	S	3/0/0
SBRG7005	GÜVENLİ SİSTEM MİMARİSİ TASARIMI	3	6	S	3/0/0

Tablo 20 (Devamı)

Kod	Ders Adı	Kredi	AKTS	Z/S	T/U/L
SBRG7002	GÜVENLİ YAZILIM TASARIMI	3	6	S	3/0/0
SBRG7000	KRİPTOGRAFİ	3	6	Z	3/0/0
SBRG7007	KRİTİK ALTYAPILARDA GÜVENLİK	3	6	S	3/0/0

Tablo 21 *İstanbul Üniversitesi Cerrahpaşa Siber Güvenlik Yüksek Lisans 1. Sınıf- Güz Dönemi Dersleri (İstanbul Üniversitesi-Cerrahpaşa, 2023b).*

Kod	Ders Adı	Kredi	AKTS	Z/S	T/U/L
SBRG7015	BULUT BİLİŞİM VE GÜVENLİK	3	6	S	3/0/0
SBRG7013	GÜVENLİ WEB YAZILIM TASARIMI	3	6	S	3/0/0
SBRG7014	MALWARE ANALİZİ	3	6	S	3/0/0
SBRG7018	SAYILAR TEORİSİ	3	6	S	3/0/0
SBRG7009	SEMİNER	0	6	Z	0/0/0
SBRG7012	SİBER GÜVENLİK HUKUKU	3	6	S	3/0/0
SBRG7011	SİBER GÜVENLİK, SALDIRI VE SAVUNMA YÖNTEMLERİ	3	6	Z	3/0/0
SBRG7016	SİBER SAVAŞ	3	6	S	3/0/0
SBRG7017	YAPAY ZEKÂ İLE GÜVENLİK	3	6	S	3/0/0

4.4.1.13. Milli Savunma Üniversitesi

Milli Savunma Üniversitesi (MSÜ), Türkiye'de askeri personel yetiştirme konusunda kritik bir rol oynayan saygın bir eğitim kurumudur. Bu üniversitede yer alan bilgisayar mühendisliği bölümü, öğrencilere güçlü bir altyapı sağlamayı ve onları bilgisayar mimarisi, mikro işlemciler, işletim sistemleri, programlama dilleri, algoritmalar, veri tabanları, yazılım mühendisliği ve bilgisayar ağları gibi çeşitli disiplinlere yönlendirmeyi amaçlamaktadır. Askeri öğrenciler, eğitim süreçleri boyunca farklı programlama dilleri ve işletim sistemleri hakkında derinlemesine bilgi edinmektedirler (Milli Savunma Üniversitesi, n.d.-a; Milli Savunma Üniversitesi, n.d.-b).

Bilgisayar mühendisliği bölümünün altında bulunan siber güvenlik programı da dikkat çekicidir. Bu programın hedefi, öğrencilere bilgisayar ve ağ güvenliği ile siber güvenlik konularında gerekli kavramsal, terminolojik ve teknik bilgileri kazandırmaktır. Ayrıca, temel teorik ve uygulamalı yöntemler hakkında güncel bilgi ve perspektifler sunmayı, alandaki son gelişmeleri takip edebilme ve elde edilen verileri yorumlayabilme yeteneklerini geliştirmeyi amaçlamaktadır. Öğrenciler, sorunları tanımlayıp çözüm üretebilme, siber güvenlik konularında bireyleri ve kurumları bilgilendirebilme, düşüncelerini ve çözüm önerilerini yazılı ve sözlü olarak ifade edebilme yetkinliklerini kazanmaktadırlar. Ayrıca, siber güvenlik alanındaki keşif ve sonuçları diğer bilim dalları ile entegre edebilme yetisine de sahip olmaktadırlar (Milli Savunma Üniversitesi, n.d.-a; Milli Savunma Üniversitesi, n.d.-b).

Milli Savunma Üniversitesi bünyesinde ATASAREN , Alp Arslan ve Hava Harp Okulu gibi enstitüler bünyesinde ayrı ayrı siber güvenlik tezli ve tezsiz yüksek lisans programları mevcuttur. Bunların açık kaynaklarından erişilen programlarda eksikler olsa da aşağıda tablolar şeklinde yer verilmiştir.

Tablo 22 *Alparslan Savunma Bilimleri ve Millî Güvenlik Enstitüsü Siber Güvenlik Yüksek Lisans Programı Dersleri (Milli Savunma Üniversitesi, n.d.-c)*

Kod	Yarıyıl	Ders Adı	Kredi	AKTS	Tür
ALP 4356	II. Yarıyıl	Seminer	-	6	Z
ALP 4357	II. Yarıyıl	Bilgi Güvenliği ve Kriptografi	3	6	Z
ALP 4364	II. Yarıyıl	Makine Öğrenmesi	3	6	S
ALP 4362	II. Yarıyıl	Siber Saldırı Teknikleri	3	6	S
ALP 4360	II. Yarıyıl	Bilgi Güvenliği ve Yönetimi	3	6	S

Tablo 23 *ATASAREN Siber Güvenlik Yüksek Lisans Programı II. Yarıyıl Zorunlu Dersler (Milli Savunma Üniversitesi, 2023)*

Ders Kodu	Ders Adı
SIG7000	Yüksek Lisans Semineri
SIG7010	Araştırma Yöntemleri ve Bilimsel Etik

Tablo 24 *ATASAREN Siber Güvenlik Yüksek Lisans Programı II. Yarıyıl Seçmeli Dersler (Milli Savunma Üniversitesi, 2023)*

Ders Kodu	Ders Adı
SIG7012	Adli Bilişim
SIG7014	Siber Savaş ve Güvenlik
SIG7034	Süreç Madenciliği ve Süreç Zekâsı
SIG7036	Sayısal Ses ve Konuşma İşleme
SIG7038	Yapay Zekâ
SIG7056	Oyunlar İçin Programlama

4.4.2. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, ASELSAN, HAVELSAN, TSK, EGM, SSB, TÜBİTAK ve BTK'nın Siber Güvenlik Eğitimi Faaliyetleri

Bu kurumların eğitim faaliyetleri, Türkiye'de siber güvenlik alanında insan kaynağının geliştirilmesine önemli katkılar sunmaktadır. TÜBİTAK ve BTK'nın düzenlediği eğitim programları ve projeler, siber güvenlik alanında yenilikçi çözümler ve teknolojiler geliştirilmesini teşvik etmektedir. Ayrıca, bu programlar, katılımcıların siber güvenlik alanındaki bilgi ve becerilerini

güncellemelerine ve sektörde gerçekleşen en son gelişmeleri kaçırmamalarına yardımcı olmaktadır (TÜBİTAK BİLGEM, 2023).

4.4.2.1.Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CDDO), Türkiye'nin dijital dönüşüm sürecini yönlendirmek ve ulusal dijital stratejilerin geliştirilmesini sağlamak amacıyla kurulmuş bir devlet kurumudur. Ofis, özellikle kamu sektörünün dijitalleşmesi, veri güvenliği, siber güvenlik ve dijital ekonomi gibi kritik alanlarda aktif rol oynamaktadır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024).

CDDO'nun temel görevler ve sorumlulukları; Dijital Dönüşüm Stratejilerinin, Geliştirilmesi, Veri Güvenliği ve Siber Güvenlik, E-Devlet Uygulamaları, Ulusal Yapay Zekâ Stratejisi ve Dijital Ekonomi ve Yenilikçi Teknolojiler olarak sıralanmaktadır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). Bu bağlamda çalışmamızın doğrudan alanına giren göre, sorumluluk ve faaliyetleri şu şekildedir:

- **Dijital Dönüşüm Stratejilerinin Geliştirilmesi:** CDDO, Türkiye'nin dijital dönüşümünü desteklemek amacıyla stratejiler oluşturur ve bu stratejilerin uygulanmasını sağlar. Ayrıca, dijitalleşme süreçlerini ulusal düzeyde koordine eder (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). Ofis, Türkiye'nin siber güvenlik altyapısını güçlendirmeyi hedefleyen çeşitli stratejik planlar geliştirmektedir. Bu stratejiler, kamu ve özel sektörün siber güvenlik kapasitelerinin artırılmasına odaklanmaktadır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024).
- **Veri Güvenliği ve Siber Güvenlik:** Ofisin bir diğer önemli görevi, dijital ortamda karşılaşılabilecek tehditlere karşı korunma sağlayacak siber güvenlik politikaları geliştirmektir. Kamu kurumlarının ihtiyaç duyduğu güvenlik standartlarının belirlenmesi ve uygulanması da bu kapsamda değerlendirilmektedir (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024).
- CDDO, dijital dönüşüm süreçlerine dahil olan tüm paydaşların dijital okuryazarlık ve dijital yetkinliklerini artırmak için eğitim programları düzenlemektedir. Ayrıca, toplum genelinde dijital dönüşüm ve siber

güvenlik konularında farkındalık yaratmak amacıyla çeşitli kampanyalar ve eğitim programları organize edilmektedir (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024).

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Cumhurbaşkanlığı'na doğrudan bağlı olarak faaliyet göstermektedir ve başkan ile başkan yardımcıları tarafından yönetilmektedir. Ofis bünyesinde, çeşitli daire başkanlıkları ve uzmanlık alanlarına göre ayrılmış birimler bulunmaktadır (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2024). Çalışma konusu alanda üst organizasyon olarak değerlendirilebilecek bu merkezi teşkilatta Siber Güvenlik Daire Başkanlığı tesis edilmiştir.

4.4.2.2.ASELSAN

ASELSAN, Türk Silahlı Kuvvetleri (TSK) başta olmak üzere müşterilerine kaliteli ürün ve çözümler sunarak ülkenin dışa bağımlılığını en aza indirmeyi amaçlayan uluslararası bir savunma elektroniği şirketidir (ASELSAN, n.d.-a; ASELSAN, n.d.-b).

Şirket, kripto ve bilgi güvenliği sistemleri, bilgi teknolojileri sistemleri, haberleşme ve bilgisayar sistemlerinde ağ güvenliği ürünleri, güvenli veri paylaşım sistemleri ve kriptolama çözümleri gibi çeşitli alanlarda çözümler sunmaktadır (ASELSAN, n.d.-a; ASELSAN, n.d.-b).

ASELSAN'ın siber güvenlik alanında birçok ürünü ve çözümü bulunmaktadır. İşte bu ürünler ve türleri:

- 2064 10G AĞ KC - IP Kripto Cihazı/Link Kripto Cihazı
- 2064 MİNİ - IP Kripto Cihazı/Link Kripto Cihazı
- 2064 RACK TİPİ KC V2 - IP Kripto Cihazı V2
- SAHAB - Sanal Hava Boşluğu
- TEK YÖNLÜ VERİ GEÇİŞ SİSTEMİ - Veri Diyodu
- SİBER ZIRH PROGRAMI - Siber Zırh Programı
- GÜVENLİK YÖNETİM MERKEZİ - Güvenlik Yönetim Merkezi
- 2080 -Anahtar Yönetim Sistemi (ASELSAN,n.d.-a; ASELSAN, n.d.-b).

4.4.2.3.HAVELSAN

HAVELSAN, Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir şirketi olarak 1982 yılında kurulmuştur. Türkiye'nin en büyük teknoloji firmalarından biri olarak kabul edilen HAVELSAN; deneyimi, uzman çalışanları ve ileri teknolojiye dayalı yazılım yoğun özgün çözüm ve ürünleriyle uluslararası arenada lider bir markadır (HAVELSAN, n.d.-a; HAVELSAN, n.d.-b).

HAVELSAN elinde hizmet olarak siber güvenlik operasyon merkezi, analiz ve test hizmetleri, danışmanlık hizmetleri ve siber güvenlik akademisi bulundurmaktadır (HAVELSAN, n.d.-a; HAVELSAN, n.d.-b).

Siber Güvenlik Operasyon Merkezi

Siber güvenlik operasyon merkezinde şu çalışmalar yürütülmektedir:

- Servis Sürekliliği ve Tehdit İzleme
- Siber Tehdit İstihbaratı
- Siber Olay İzleme, Analizi ve Danışmanlığı
- Siber Olay Müdahale ve Yönetimi
- Adli Bilişim Analizi ve Zararlı Yazılım İncelemesi
- Teknik İnceleme ve Raporlama (HAVELSAN, n.d.-a).

Analiz ve Test Hizmetleri

Analiz ve test hizmetlerinde şu hizmetler sunulmaktadır:

- Zafiyet Denetimi: Kurum ağlarının güvenliğini sağlama
- Sızma Testi: Kurum sistemlerinin güvenlik açıklarını tespit etme ve raporlama
- Uygulama/Kaynak Kod Güvenlik Analizi: Yazılımların güvenlik zafiyetlerini koruma
- Bilişim Sistemleri Güvenlik Denetimi: Bilgi sistemlerinin güvenliğini kontrol etme (HAVELSAN, n.d.-a).

Danışmanlık Hizmetleri

Danışmanlık hizmetleri olarak Siber Olgunluk Seviyesi Belirleme Testi sunulmaktadır. Bu test, olası saldırılara karşı mevcut durumları önceden belirleyip hızlı ve etkin tedbir alınmasını sağlar (HAVELSAN, n.d.-a).

Siber Güvenlik Akademisi

Siber güvenlik akademisi, katılımcıların becerilerini geliştirmek ve alan uzmanlığı sağlamak için farklı yetkinlik seviyelerine özel eğitimler sunar. Eğitimler üç seviyeye ayrılır:

- **Temel Seviye Eğitimler:**
  - Siber Güvenlik Farkındalık Eğitimi
  - Siber Güvenlik Temelleri
  - Yöneticiler İçin Siber Güvenlik Semineri
  - Siber Saldırı ve Savunamaya Giriş
  - Temel Seviye Siber Olay Yönetimi ve Müdahale
  - Ağ Güvenliği Temelleri
  - İşletim Sistemleri Güvenlik Sıkılaştırma
- **Orta Seviye Eğitimler:**
  - Ağ Zafiyet Taraması ve Sızma Testi
  - Web Uygulama Zafiyet Taraması ve Sızma Testi
  - Kötücül Yazılım Analizi Temelleri
  - Mobil Güvenlik
  - Güvenli Yazılım Geliştirme Temelleri
  - Etkin SIEM Kullanım
  - HAVELSAN Kalkan - Web Uygulama Güvenlik Duvarı Yönetimi
- **Uzman Seviye Eğitimler:**
  - Endüstriyel Kontrol Sistemleri Güvenliği
  - Bilişim Sistemleri Güvenlik Denetimi
  - İleri Seviye Ağ Sızma Testi ve Zafiyet Denetimi
  - İleri Seviye Web Uygulama Saldırıları ve Koruma
  - Kırmızı ve Mavi Takım Eğitimleri
  - Siber Tehdit İstihbaratı (HAVELSAN, n.d.-a).

Ürünler

HAVELSAN'ın siber güvenlik alanında geliştirdiği ürünler şunlardır:

- **HAVELSAN KALKAN:** Yüzde yüz milli imkanlar ile geliştirilmiş bir Yük Dengeleme/Web Uygulama Güvenlik Duvarı.
- **HAVELSAN BARİYER:** PARDUS ile uyumlu, veri sızıntısı önleme (DLP) ürünü.
- **HAVELSAN İleti:** Güvenli iletişim uygulaması.
- **HAVELSAN Veri Diyotu:** Hassas veri barındıran izole ağlar için geliştirilmiş veri aktarım çözümü (HAVELSAN, n.d.-b).

4.4.2.4.Türk Silahlı Kuvvetleri (TSK)

Türk Silahlı Kuvvetleri (TSK), siber güvenlik alanında kapsamlı eğitim faaliyetleri ve tatbikatlar düzenlemekte, bu faaliyetleri sürekli olarak geliştirmekte ve modernize etmektedir. Bu kapsamda, Türkiye'nin siber güvenlik stratejisinin bir parçası olarak çeşitli organizasyonlar ve tatbikatlar gerçekleştirilmektedir. TSK, özellikle Milli Savunma Üniversitesi bünyesinde kurduğu Siber Savunma Merkezi Komutanlığı ile siber güvenlik eğitimleri düzenlemektedir. Bu merkezde, askeri personelin yanı sıra sivil katılımcılara da yönelik ileri düzey siber güvenlik eğitimleri verilmektedir. Eğitimler, hem teorik hem de pratik uygulamaları kapsayacak şekilde yapılandırılmıştır. Ayrıca, TSK, NATO'nun siber güvenlik merkezi CCDCOE ile iş birliği yaparak uluslararası düzeyde de siber güvenlik tatbikatlarına katılmaktadır (CCDCOE, 2021; Halisdemir, 2021).

TSK'nın düzenlediği siber güvenlik tatbikatları arasında, geniş çaplı ve çok uluslu tatbikatlar yer almakta olup, bu tatbikatlar genellikle NATO ile koordinasyon halinde gerçekleştirilmektedir. Bu tatbikatlar, TSK'nın siber savunma kapasitesini artırmak ve uluslararası iş birliğini güçlendirmek amacıyla yapılmaktadır. Ayrıca, Türkiye'nin 2023 Ulusal Siber Güvenlik Stratejisi çerçevesinde, TSK'nın siber güvenlik alanındaki organizasyon ve faaliyetleri, kritik altyapıların korunması, siber saldırılara karşı hızlı tepki verilmesi ve siber güvenlik kültürünün yaygınlaştırılması gibi hedefler doğrultusunda şekillendirilmektedir (Invest in Turkey, 2023).

Bu organizasyonlar ve tatbikatlar, Türkiye'nin siber savunma kabiliyetlerini ulusal ve uluslararası düzeyde güçlendirmeye yönelik önemli adımlar olarak değerlendirilmektedir. Türkiye'nin siber güvenlik stratejisi ve TSK'nın bu alandaki rolü, hem ulusal güvenliği sağlamak hem de uluslararası iş birliğini geliştirmek açısından kritik bir öneme sahiptir (Invest in Turkey, 2023; CCDCOE, 2021).

4.4.2.5.Savunma Sanayii Başkanlığı (SSB) Siber Güvenlik Kümelenmesi

Savunma Sanayi Akademi (SSA), Türk savunma sanayii için nitelikli insan kaynağı yetiştirmeyi hedefleyen ve sektöre özel tasarlanmış öğrenme deneyimleri sunan bir kurumdur. Bu akademi, öğrenenlerin yerli ve milli kaynaklarla ekosisteme katkı sağlamasını amaçlar (Savunma Sanayii Akademisi, 2024-a).

Türkiye Siber Güvenlik Kümelenmesi

Türkiye Siber Güvenlik Kümelenmesi (TSGK), 2017 yılında Savunma Sanayii Başkanlığı ve Dijital Dönüşüm Ofisi Başkanlığı desteğiyle kurulmuş ve SSTEK A.Ş. tarafından yürütülen bir projedir. Bu kümelenme, kamu, özel sektör ve akademiyi bir araya getirerek siber güvenlik ekosistemini geliştirmeyi hedefler. Misyonu, yenilikçi yöntemlerle ihtiyaçları karşılayarak siber güvenlikte iş birliği ve rekabet ortamı yaratmaktır. Vizyonu ise, üyelerinin küresel ve yerel pazarda rekabet gücünü artırmaktır (Türkiye Siber Güvenlik Kümelenmesi, n.d.-a).

Günümüz dünyasında, bilgi güvenliğinin sağlanması en az sınır güvenliği kadar önemli hale gelmiştir. Siber saldırılar gün geçtikçe daha karmaşık ve hedef odaklı bir hal almaktadır. Bu saldırıların ve potansiyel tehditlerin anlaşılması, bu tehditlere karşı önlemler geliştirilmesi amacıyla Siber Güvenlik kavramı, tüm devlet kurumlarının öncelikli gündem maddeleri arasında yer almaktadır. Bu bağlamda, Savunma Sanayii Akademisi, sektörde yetkin paydaşların katkılarıyla, farkındalık seviyesinden başlayarak temel, ileri ve uzmanlık düzeylerine kadar geniş bir yelpazede uygulamalı ve kapsamlı bir eğitim müfredatı oluşturmuştur (Savunma Sanayii Akademisi, 2024-b).

Hedefler

- Türkiye'deki siber güvenlik firmalarının sayısını artırmak
- Üyelerin teknik, idari ve finansal açılardan gelişimine destek olmak
- Siber güvenlik ekosisteminin standartlarını geliştirmek
- Üyelerin ürün ve hizmetlerinin markalaşmasına yardımcı olmak
- Üyelerin ulusal ve küresel pazarda rekabet gücünü artırmak
- Siber güvenlik alanındaki insan kaynağı sayısı ve niteliğini artırmak
- Toplumdaki siber güvenlik bilincini artırmak

TSGK, Türkiye'deki siber güvenlik ekosistemini güçlendirmek amacıyla kariyer fırsatları sunarak sektörde istihdamı teşvik etmektedir. Bu girişimler, sektördeki yetenek açığını kapatarak ulusal güvenliğe katkı sağlar (Türkiye Siber Güvenlik Kümelenmesi, n.d.-b).

TSGK, gençlerin siber güvenliğe olan ilgisini artırmak ve ekosistemin ihtiyaçlarını karşılamak amacıyla düzenli olarak yaz ve kış kampları, gece eğitim programları ve yarışmalar düzenler. Ayrıca, çevrim içi eğitim serileri ve sızma testi eğitimleri gibi programlar da sunmaktadır (Türkiye Siber Güvenlik Kümelenmesi, n.d.-c).

TSGK, siber güvenlik alanında faaliyet gösteren kuruluşları çeşitli şekillerde destekler. Bu destekler arasında katalog sunma, etkinlik düzenleme, eğitim programları sunma ve araştırma-geliştirme faaliyetleri yer alır (Türkiye Siber Güvenlik Kümelenmesi, n.d.-d).

Savunma Sanayii Akademisinin (SSA) Eğitim Programlarındaki Eğitim Modülleri (Savunma Sanayii Akademisi, 2024-b):

Tablo 25 *SSA Farkındalık Seviyesi Siber Güvenlik Eğitim Modülleri* (Savunma Sanayii Akademisi, 2024-b)

Modül Kodu	Modül Adı
FS1	Bilgi Güvenliği Temelleri
FS2	ISO27001 Bilgi Güvenliği Yönetimi Sistemi (BGYS)

Tablo 25 (Devamı)

Modül Kodu	Modül Adı
FS3	Risk Değerlendirme, İş Sürekliliği ve Felaketten Kurtarma
FS4	Temel Açık Kaynak ve Siber Tehdit İstihbaratı

Tablo 26 *SSA Temel Seviye Siber Güvenlik Eğitim Modülleri (Savunma Sanayii Akademisi, 2024-b)*

Modül Kodu	Modül Adı
TS1	Siber Güvenlik Temel Kavramlar ve Teknolojiler
TS2	Linux Güvenliğine Giriş
TS3	Ağ Güvenliğine Giriş
TS4	Windows Güvenliği Giriş
TS5	Web Uygulama ve Veri Tabanı Güvenliği
TS6	SOME Kurulumu ve Yönetimi

Tablo 27 *SSA İleri Seviye Siber Güvenlik Eğitim Modülleri (Savunma Sanayii Akademisi, 2024-b)*

Modül Kodu	Modül Adı
İS1	Siber Güvenlik Operasyon Merkezi
İS2	Siber Güvenlik Sistemleri Yönetimi
İS3	İleri Sızma Testi

Tablo 27 (Devamı)

Modül Kodu	Modül Adı
İS4	İleri Adli Bilişim
İS5	Yazılım-Uygulama Güvenliği
İS6	Siber Güvenlik Yönetişimi
İS7	İleri Zararlı Yazılım Analizi

Tablo 28 *SSA Uzman Seviye Siber Güvenlik Eğitim Modülleri (Savunma Sanayii Akademisi, 2024-b)*

Modül Kodu	Modül Adı
US1	Uzman Zararlı Yazılım Analizi
US2	Uzman Adli Analiz
US3	Açıklık Geliştirme
US4	Siber Güvenlik Büyük Veri Bilimi

4.4.2.6.Emniyet Genel Müdürlüğü (EGM)

Emniyet Genel Müdürlüğü'nün (EGM) bünyesinde yer alan Siber Suçlarla Mücadele Daire Başkanlığı, bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek sağlayan çeşitli il birimlerini bir araya getirmiştir (Emniyet Genel Müdürlüğü, 2022; Emniyet Genel Müdürlüğü, n.d.). Bu daire başkanlığı, değişen ve gelişen dünya koşulları çerçevesinde geleceğe yönelik bir vizyonla hareket etmektedir. Amacı, siber suçlarla mücadelede uzmanlaşmış, fikirlerin özgürce ifade edildiği, dinamik ve eşitlikçi bir yönetim anlayışına sahip, yüksek ahlaki değerlere bağlı ve 'güven' kelimesiyle özdeşleşen bir kurum kültürü oluşturmaktır.

Siber Suçlarla Mücadele Daire Başkanlığı'nın diğer amaçları ise şu şekilde sıralanabilir:

1. Siber suçlarla etkin bir şekilde mücadele etmek,
2. Toplumda siber suçlar konusunda farkındalık yaratmak,
3. Uluslararası iş birliklerini artırarak siber suçlarla mücadeleyi güçlendirmek,
4. Ülkeye yönelik siber tehditleri değerlendirmek, gerekli analizleri yapmak ve bu tehditlerle başa çıkmak,
5. Siber suçlarla mücadelede uzman soruşturmacılar ve adli bilişim personeli yetiştirmek,
6. Teknolojik gelişmeleri takip etmek ve bu teknolojileri kullanarak siber suçlarla mücadele kapasitesini artırmak.

Bu hedefler, Emniyet Genel Müdürlüğü'nün siber suçlarla mücadelede izlediği stratejinin temel taşlarını oluşturmaktadır (Emniyet Genel Müdürlüğü, 2022; Emniyet Genel Müdürlüğü, n.d.).

SİBERAY

Emniyet Genel Müdürlüğü tarafından yürütülen Siberay Projesi, Türkiye'nin siber güvenlik eğitimi politikasının önemli bir parçasını teşkil etmektedir. Bu girişim, siber güvenlik farkındalığını artırarak vatandaşları dijital tehditlere karşı korumayı hedeflemektedir (Emniyet Genel Müdürlüğü, 2021). Proje, bireyler ve kurumlar için eğitim programları, seminerler ve farkındalık kampanyaları düzenleyerek siber güvenlik konusundaki bilgi düzeyini yükseltmektedir. Siberay Projesi'nin detayları ve eğitim politikası kapsamındaki değerlendirmesi aşağıda sunulmuştur.

Projenin Amacı ve Kapsamı

Siberay Projesi, toplumun tüm kesimlerinde siber güvenlik bilincini artırmayı amaçlayan bir girişimdir. Emniyet Genel Müdürlüğü tarafından hayata geçirilen bu proje, bireylere ve kurumlara yönelik çeşitli eğitim ve bilinçlendirme faaliyetlerini içermektedir. Çocuklar, gençler, yetişkinler ve kamu çalışanları için farklı modüller ve eğitim materyalleri hazırlanmıştır (Emniyet Genel Müdürlüğü, 2021).

Eğitim Modülleri ve İçerikler

Proje kapsamında sunulan eğitimler, temel siber güvenlik bilgileri, güvenli internet kullanımı, veri koruma, sosyal mühendislik saldırıları, zararlı yazılımlar ve siber zorbalık gibi konuları içermektedir. Bu eğitimler, interaktif seminerler, çevrimiçi kurslar ve farkındalık kampanyaları şeklinde sunulmaktadır.

Projenin Hedef Kitlesi ve Yaygınlaştırma Stratejisi

Projenin hedef kitlesi oldukça geniştir. Okullarda öğrencilere yönelik düzenlenen eğitimler, ebeveynlere yönelik bilinçlendirme seminerleri ve kamu çalışanlarına özel eğitim programları bulunmaktadır. Ayrıca, sosyal medya ve diğer dijital platformlar üzerinden yürütülen kampanyalarla geniş kitlelere ulaşılmaktadır (Emniyet Genel Müdürlüğü, 2021).

Türkiye'nin Siber Güvenlik Eğitimi Politikası ile Uyumu

Siberay Projesi, Türkiye'nin genel siber güvenlik stratejisinin bir parçası olarak, ulusal güvenlik politikalarıyla uyumlu şekilde yürütülmektedir. Milli Eğitim Bakanlığı, TÜBİTAK ve diğer ilgili kurumlarla iş birliği yapılarak eğitim materyallerinin geliştirilmesi ve projelerin yaygınlaştırılması sağlanmaktadır. Bu iş birlikleri, siber güvenlik eğitimlerinin ulusal müfredata entegrasyonunu ve sürdürülebilirliğini desteklemektedir.

4.4.2.7.Türkiye Bilimsel ve Teknolojik Araştırma Kurumu-TÜBİTAK

TÜBİTAK, siber güvenlik alanında birbirinden farklı projeler ve eğitim programları düzenlemekte ve bu alanda araştırmalar yapmaktadır. TÜBİTAK'ın düzenlediği Siber Güvenlik Yaz Okulu, öğrencilere ve profesyonellere kapsamlı bir eğitim programı sunmakta ve onların siber güvenlik becerilerini geliştirmelerine yardımcı olmaktadır. Ayrıca, TÜBİTAK tarafından desteklenen çeşitli projeler, siber güvenlik alanında yenilikçi çözümler ve teknolojiler geliştirilmesini sağlamaktadır (TÜBİTAK BİLGEM, 2023).

Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi-BİLGEM

Türkiye'nin en yetkin Ar-Ge merkezi olma özelliği taşıyan BİLGEM, ülkemizin bilgi güvenliği ve bilişim alanında teknolojik bağımsızlığını kazanması için araştırma ve geliştirme (Ar-Ge) çalışmaları gerçekleştirmektedir (TÜBİTAK BİLGEM, 2024).

BİLGEM'in bünyesinde siber güvenlik, blokzincir, e-kimlik teknolojileri, yazılım geliştirme, veri teknolojileri, kriptoloji, açık anahtar yapısı, kuantum teknolojileri, dijital dönüşüm, yarı iletken teknolojileri, mesajlaşma sistemleri, algılayıcı teknolojiler, biyoelektronik, Coğrafi Bilgi Sistemleri (GIS) ve aviyonik teknolojiler, deniz savunma ve su altı akustik, güvenli haberleşme, elektro-optik ve lazer ve elektromanyetik sistemler gibi alanlar bulunmaktadır (TÜBİTAK BİLGEM, 2024).

BİLGEM'in siber güvenlik alanında gerçekleştirdiği bazı önemli çalışmalar arasında ORION (Veri Güvenlik Platformu), DERBENT (Güvenli Uzaktan Erişim Sistemi), SİBERLAB (Sanal Siber Güvenlik Laboratuvarı), BOT-SEGEN (Bilişim ve Otomasyon Teknolojileri Sızma Testi ve Güvenlik Denetimi Platformu), A3 (Adli Analiz Altyapısı) ve MERGE-N (Entegre Uç Birim Güvenlik Platformu) bulunmaktadır (TÜBİTAK BİLGEM, 2024).

ORION, hassas verilerin olası izinsiz erişim senaryolarına karşı koruma sağlayan bir yazılımdır. DERBENT, güvenli bir şekilde uzaktan erişim sağlamayı hedefleyen yerli bir projedir. SİBERLAB, bulut üzerinde hızlı, kolay ve düşük maliyetle siber güvenlik eğitimi, test, tatbikat ve siber güvenlik analizi gibi faaliyetleri gerçekleştirmeyi amaçlayan bir projedir. BOT-SEGEN, derin uzmanlık bilgisine sahip olmadan tek bir platform üzerinden sızma testi ve güvenlik denetimini otomize ederek kullanıcıların zaman ve maliyet tasarrufu sağlamasını hedefleyen bir projedir. A3, çeşitli elektronik aygıtların adli analizlerde incelenmesini kolaylaştıran bir projedir. MERGE-N ise yerli siber güvenlik ürünlerinin güvenli bir şekilde tanıtımını amaçlayan bir web uygulamasıdır (TÜBİTAK BİLGEM, 2024).

Siber Güvenlik Eğitim Portalı - SGEP

Siber Güvenlik Eğitim Portalı, Kalkınma Bakanlığı iş birliği ile TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü tarafından yürütülen Siber Güvenlik Eğitim

ve Araştırma Merkezi Projesi – Siber Güvenlik Eğitim Altyapısı iş paketi kapsamında hayata geçirilmiştir (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

Siber Güvenlik Eğitim Portalının amacı, toplumun siber güvenlik alanı hakkında bilgilendirilmesi, yükseköğretim öğrencilerinin bu konu hakkında teknik bilgi elde edebilmesi ve bu alanda çalışan uzmanların yetkinliklerinin genişlemesidir (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

Siber Güvenlik Eğitim Portalında beş adet eğitim kataloğu bulunur. Bunlar sırasıyla bilgi güvenliği yönetimi eğitimleri, güvenlik testleri ve denetimi eğitimleri, güvenlik analizi eğitimleri, sistem ağ ve güvenliği eğitimleri ve uygulama güvenliği kataloglarıdır (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

Bilgi güvenliği eğitimleri kataloğunda altı adet ders bulunmaktadır. Bunlar sırasıyla kullanıcı güvenliği, yöneticilere odaklı genel güvenlik, ISO 27001 bilgi güvenliği yönetim sistemi uygulamaları, yöneticilere odaklı ISO 27001 bilgilendirme, siber olaylara müdahale ekibi ve kritik altyapıların korunması dersleridir (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

Güvenlik testi ve denetimi eğitimleri kataloğunda yedi adet ders bulunmaktadır. Bunlar sırasıyla sosyal mühendislik: saldırı ve korunma yöntemleri, bilgi güvenliğine giriş, sistem güvenlik denetimi, temel güvenlik denetimi, sızma testi uzmanlığı, DDoS saldırıları ile mücadele ve ileri sızma testi uzmanlığı dersleridir (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

Güvenlik analizi eğitimleri kataloğunda beş adet ders bulunmaktadır. Bunlar sırasıyla kayıt yönetimi, kayıt analizi, temel bilgisayar analizi, ağ trafik analizi ve Windows zararlı yazılım analizi dersleridir (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

Sistem ağ ve güvenlik eğitimleri kataloğunda yedi adet ders bulunmaktadır. Bunlar sırasıyla Windows güvenliği, Microsoft sistemleri güvenliği, Linux güvenliği, TCP/IP ağ güvenliği, aktif cihaz güvenliği, kablosuz ağ güvenliği ve merkezi kayıt yönetim sistemleri dersleridir (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

Uygulama güvenliği eğitimleri kataloğunda beş adet ders bulunmaktadır. Bunlar sırasıyla Oracle veritabanı güvenliği, MS SQL Server veritabanı güvenliği, web uygulamaları güvenliği, mobil güvenlik ve güvenli yazılım geliştirme dersleridir (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

TÜBİTAK, son 20 yılda siber güvenlik alanında toplamda 664 projeye yaklaşık 1 milyar lira destek verdiğini belirtmektedir. Bu alanda yeni girişimcilerin ortaya çıkmasını destekleyen Sanayi ve Teknoloji Bakanı Varank, bu gelişmelerin yeni girişimcilerin çıkmasına büyük katkı sağladığını ifade etmiştir (TÜBİTAK, 2022).

Siber Güvenlik Eğitim Portalı, ücretsiz eğitimler sunmanın yanı sıra, bu eğitimlerin tamamlanması karşılığında öğrencilere e-posta aracılığıyla bilgilendirme yaparak çeşitli alanlarda ihtiyaç duyulan ve fayda sağlayacak sertifikalar vermektedir (TÜBİTAK, n.d.-a; Siber Güvenlik Eğitim Portalı, n.d.-a).

4.4.2.8.Bilgi Teknolojileri ve İletişim Kurumu-BTK

BTK siber güvenlik eğitimi alanında önemli faaliyetler yürütmektedir. BTK'nın Siber Yıldız Programı, siber güvenlik uzmanları yetiştirmek amacıyla çeşitli eğitimler ve yarışmalar düzenlemektedir. Bu program, öğrencilere ve profesyonellere siber güvenlik alanında pratik deneyimler sunmakta ve onların bu alanda yetkinlik kazanmalarını sağlamaktadır. Ayrıca, BTK tarafından düzenlenen siber güvenlik seminerleri ve konferanslar, katılımcıların siber güvenlik konusundaki bilgilerini güncellemelerine ve sektördeki gelişmeleri takip etmelerine olanak tanımaktadır (CoHE, 2023).

BTK Akademi, kullanıcılarına ücretsiz, güvenilir ve güncel eğitim sunan bir elektronik öğrenme platformudur. 2017 yılında T.C. Ulaştırma ve Altyapı Bakanlığı Bakan Yardımcısı Dr. Ömer Fatih Sayan'ın öncülüğünde kurulmuştur (BTK Akademi, n.d.-a). BTK Akademi, her yaş ve milletten insanlara, Türkiye'de okuma şartıyla, çeşitli konularda ücretsiz bilgi ve beceri kazandırmaktadır; bunlar arasında siber güvenlik de yer almaktadır (BTK Akademi, n.d.-a).

Siber güvenlik alanında, BTK Akademi'de dört ana konu başlığı bulunmaktadır: siber güvenlik uzmanlığı, sızma testi uzmanlığı, adli bilişim uzmanlığı ve zararlı yazılım uzmanlığı. Bu alanlarda toplamda 35 ders sunulmaktadır: siber güvenlik uzmanlığı için 10 ders, sızma testi uzmanlığı için 13 ders, adli bilişim uzmanlığı için 8 ders ve zararlı yazılım uzmanlığı için 4 ders (BTK Akademi, n.d.-a).

BTK Akademi Siber Güvenlik Dersleri

Siber Güvenlik Uzmanlığı Dersleri

Tablo 29 *Siber Güvenlik Uzmanlığı Dersleri (BTK Akademi, 2021)*

Ders Adı	Durum
Siber Güvenliğe Giriş	Aktif
Bilişim Hukuku	Aktif
Log Analizi	Hazırlanmakta
Network Analizi	Hazırlanmakta
Bellek Taşma Açıklıkları ve Exploit Geliştirme	Aktif
Malware Geliştirme ve Malware Analizi	Hazırlanmakta
Siber Güvenlik Analisti	Aktif
Güvenlik Testi	Aktif
Python ile Siber Güvenlik Uygulamaları	Aktif

Sızma Testi Uzmanlığı Dersleri

Tablo 30 *Sızma Testi Uzmanlığı Dersleri (BTK Akademi, 2021)*

Ders Adı	Durum
Siber Güvenliğe Giriş	Aktif
Bilişim Hukuku	Aktif
İleri Ağ Güvenliği	Hazırlanmakta
İleri Web Güvenliği ve Web Sızma Teknikleri	Hazırlanmakta

Tablo 30 (Devamı)

Ders Adı	Durum
Uygulamalı Sızma Testi	Aktif
Web Uygulama Güvenliği	Aktif
Veritabanı Güvenliği	Aktif
Bellek Taşma Açıklıkları ve Exploit Geliştirme	Aktif
Mobil Güvenlik ve Sızma Teknikleri	Aktif
Güvenlik Testi	Aktif
Kablosuz Ağ Güvenliği	Aktif
Zafiyet Araştırma ve Ağ Güvenliği	Hazırlanmakta
Python ile Siber Güvenlik Uygulamaları	Aktif

Adli Bilişim Uzmanlığı Dersleri

Tablo 31 *Adli Bilişim Uzmanlığı Dersleri (BTK Akademi, 2021)*

Ders Adı	Durum
Siber Güvenliğe Giriş	Aktif
Bilişim Hukuku	Aktif
Log Analizi	Hazırlanmakta
Network Analizi	Hazırlanmakta
Mobil Forensic+	Hazırlanmakta
Linux Forensic+	Hazırlanmakta
Windows Forensic+	Hazırlanmakta
Adli Bilişime Giriş	Aktif

Zararlı Yazılım Uzmanlığı Dersleri

Tablo 32 *Zararlı Yazılım Uzmanlığı Dersleri (BTK Akademi, 2021)*

Ders Adı	Durum
Siber Güvenliğe Giriş	Aktif
Bilişim Hukuku	Aktif
Tersine Mühendislik	Hazırlanmakta
Malware Geliştirme ve Malware Analizi	Hazırlanmakta

BTK Akademi, kamu kurumlarının siber alanda kendilerini geliştirmeleri için Ulusal Siber Kalkan 2021 ve 2022 tatbikatlarını başlatmış ve burada ödüller vermiştir (BTK Akademi, 2021). BTK Akademi, 2024 yılında düzenlenen 8. Hacktrick Siber Güvenlik Konferansı'na ev sahipliği yapmış ve yine 2024 yılında 7. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi'ni düzenlemiştir. (BTK Akademi, 2024).

WatchGuard Tehdit Laboratuvarı'na göre Türkiye, saatte 115 siber saldırı ile pek çok hacker ve ülkenin hedefi konumundadır. KASIRGA, AVCI, AZAD, ATMACA ve KULE gibi yazılımlar, ülkemizin siber güvenlik alanında dikkate değer bir korunma sağladığını göstermektedir. Bu yazılımların geliştirilmesinde çalışacak insanları yetiştirmede BTK Akademi büyük bir rol üstlenmektedir (BTK Akademi, 2024).

4.4.2.9.Özel Sektör ve STK'ların Siber Güvenlik Eğitimine Katkıları

Özel sektör ve STK'lar, Türkiye'de siber güvenlik eğitimine önemli katkılar sunmaktadır. Büyük teknoloji firmaları ve güvenlik şirketleri, çalışanlarına yönelik kapsamlı siber güvenlik eğitim programları düzenlemekte ve bu alanda uzmanlaşmalarını sağlamaktadır (CCDCOE, 2018). Ayrıca, özel sektör tarafından sunulan sertifikasyon programları, profesyonellerin siber güvenlik alanındaki yetkinliklerini artırmalarına yardımcı olmaktadır (Spoclearn, 2024). Örneğin, Cisco, Microsoft ve IBM (International Business Machines Corporation) gibi şirketler tarafından sunulan siber güvenlik eğitim programları, profesyonellere global standartlarda bilgi ve beceri kazandırmaktadır (Cisco, 2023).

STK'lar da siber güvenlik eğitimine önemli katkılar sunmaktadır. Özellikle, siber güvenlik farkındalığını artırmak amacıyla düzenlenen seminerler, konferanslar ve eğitim programları, katılımcıların siber güvenlik konusundaki bilgilerini güncellemelerine ve sektördeki gelişmeleri takip etmelerine olanak tanımaktadır (TBD, 2023). Ayrıca, STK'lar tarafından yürütülen projeler, siber güvenlik alanında yenilikçi çözümler ve teknolojiler geliştirilmesini teşvik etmektedir (TBD, 2023). Örneğin, TBD eliyle düzenlenen siber güvenlik eğitim programları, öğrencilere ve profesyonellere kapsamlı bir eğitim sunmaktadır (TBD, 2023).

Bu eğitim programları, siber güvenlik farkındalığını artırmanın yanı sıra, katılımcılara pratik deneyimler kazandırmayı hedeflemektedir. STK'lar ve özel sektör, siber güvenlik alanında insan kaynağının geliştirilmesine ve bu sektörde kariyer planlayan bireylerin yetkinliklerini artırmalarına katkıda bulunmaktadır (Spoclearn, 2024). Ayrıca, bu programlar, siber güvenlik alanında bilgi ve becerilerin sürekli olarak güncellenmesini ve geliştirilmesini sağlamaktadır (Cisco, 2023).

Özel sektör ve STK'ların siber güvenlik eğitimine katkıları, Türkiye'nin siber güvenlik ekosisteminin güçlenmesine önemli katkılarda bulunmaktadır. Bu iş birlikleri sayesinde, siber güvenlik alanında yetkin profesyoneller yetiştirilmekte ve Türkiye'nin siber tehditler karşısında daha mukavemetli hale gelmesi sağlanmaktadır (CCDCOE, 2018). Ayrıca, bu programlar, siber güvenlik alanında yenilikçi çözümler ve teknolojiler geliştirilmesini teşvik etmektedir (TBD, 2023).

Bu eğitim programlarının yanı sıra, STK'lar ve özel sektör tarafından düzenlenen yarışmalar ve hackathonlar, katılımcıların siber güvenlik alanında pratik deneyimler kazanmalarına ve yeteneklerini sergilemelerine olanak tanımaktadır (Cisco, 2023). Bu tür etkinlikler, siber güvenlik alanında yenilikçi fikirlerin ve çözümlerin ortaya çıkmasını sağlamaktadır.

4.4.3. Türkiye Cumhuriyeti Milli Eğitim Bakanlığı Uhdesindeki Kurumlarda ve Okullardaki Siber Güvenlik Eğitimi Faaliyetleri, Müfredatı ve Programları

T.C. MEB, siber güvenlik eğitimini yaygınlaştırmak ve gençleri bu alanda bilinçlendirmek amacıyla çeşitli faaliyetler, müfredatlar ve programlar düzenlemektedir. MEB, ilköğretim basamağından başlayarak ortaöğretim ve tabii ki mesleki ve teknik eğitim verdiği kurumlarında aynı zamanda kurum personeli açısından hizmet içi eğitimlerinde siber güvenlik konularına yer vermektedir. Bu programlar, öğrencilerin dijital dünyada güvenliği sağlamaları ve siber tehditlere karşı bilinçlenmeleri amacıyla tasarlanmıştır (EC-Council, 2024).

Milli Eğitim Bakanlığı özelinde en önemli uygulama yıllar süren toplantı, çalıştay ve kurumlar arası iş birlikleri neticesinde İstanbul'da Türkiye'nin ilk siber güvenlik temalı meslek lisesi olan *Teknopark Mesleki ve Teknik Anadolu Lisesi*'dir. (Teknopark İstanbul MTAL, 2024).

4.4.3.1. Ortaöğretim Düzeyinde Siber Güvenlik Eğitimi

Ortaöğretim düzeyinde, Bilgi Teknolojileri ve Yazılım dersi kapsamında siber güvenlik konularına yer verilmektedir. Bu dersler, öğrencilere temel bilgi güvenliği kavramlarını, siber tehditleri ve bunlara karşı alınabilecek tedbirleri öğretmeyi amaçlamaktadır (Daily Sabah, 2023). Ayrıca, MEB tarafından düzenlenen çeşitli projeler ve yarışmalar, öğrencilerin siber güvenlik konusundaki farkındalıklarını artırmayı hedeflemektedir (Insight Turkey, 2023).

4.4.3.2. Mesleki ve Teknik Eğitim Kurumlarında Siber Güvenlik

MEB bünyesindeki mesleki ve teknik eğitim kurumlarında, bilişim teknolojileri alanında eğitim alan öğrenciler için özel siber güvenlik programları ve müfredatlar bulunmaktadır. Bu programlar, öğrencilerin siber güvenlik alanında uzmanlaşmalarını ve bu alanda kariyer yapmalarını desteklemektedir (EC-Council, 2024). Özellikle, bilişim teknolojileri bölümlerinde ağ güvenliği, kriptografi, etik hacking ve siber tehdit istihbaratı gibi konular öğretilmektedir (Daily Sabah, 2023).

4.4.3.3.MEB'in Düzenlediği Eğitim Programları ve Projeler

MEB, siber güvenlik eğitimini desteklemek amacıyla çeşitli projeler ve eğitim programları düzenlemektedir. Bu programlar, öğretmenlerin ve öğrencilerin siber güvenlik konusundaki bilgilerini güncellemelerini ve bu alanda yetkinlik kazanmalarını sağlamaktadır (Insight Turkey, 2023). Ayrıca, MEB tarafından düzenlenen seminerler ve çalıştaylar, öğretmenlerin siber güvenlik konularında daha donanımlı olmalarına katkıda bulunmaktadır (EC-Council, 2024).

4.4.3.4.Siber Güvenlik Farkındalık Kampanyaları

MEB, siber güvenlik farkındalığını artırmak amacıyla çeşitli kampanyalar düzenlemektedir. Bu kampanyalar, öğrencilere ve velilere siber tehditler konusunda bilgi vermeyi ve güvenli internet kullanımı alışkanlıklarını kazandırmayı hedeflemektedir (Daily Sabah, 2023). Ayrıca, MEB tarafından yayımlanan kılavuzlar ve broşürler, siber güvenlik konusundaki farkındalığı artırmayı amaçlamaktadır (Insight Turkey, 2023).

4.4.3.5.Öğretmen Eğitimi ve Gelişimi

Siber güvenlik eğitiminin etkin düzeyde aktarılabilmesi için öğretmenlerin bu alanda yeterli birikime sahip olmaları gerekmektedir. MEB, öğretmenlerin siber güvenlik konusundaki bilgi ve becerilerini geliştirmek amacıyla çeşitli hizmet içi eğitim programları düzenlemektedir (EC-Council, 2024). Bu eğitimler, öğretmenlerin siber güvenlik konusunda güncel bilgilere sahip olmalarını ve öğrencilere daha etkili bir eğitim vermelerini sağlamaktadır (Daily Sabah, 2023).

4.4.3.6.Türkiye'de MEB Bünyesinde Düzenlenen Siber Güvenlik Çalıştayları ve Önemi

Türkiye'de dijital güvenliğin sağlanması, toplumsal farkındalığın artırılması ve siber güvenlik konusunda nitelikli bireyler yetiştirilmesi amacıyla gerçekleştirilen çalıştaylar, bu hedeflere ulaşmada önemli bir rol oynamaktadır. İstanbul İl Milli Eğitim Müdürlüğü tarafından düzenlenen "Siber Güvenlik ve Sosyal Medyanın Doğru Kullanımı Çalıştayları", bu çerçevede öne çıkan etkinlikler arasında yer almaktadır. Bu çalıştaylar, siber güvenlik alanındaki güncel gelişmelerin ve tehditlerin tartışıldığı, katılımcıların bilinçlendirilmesi ve eğitilmesi amacıyla düzenlenmiştir.

- **Çalıştayların Amacı ve Katılımcılar**

Çalıştayların temel amacı, siber güvenlik konusunda toplumsal farkındalık oluşturmak, sosyal medya kullanımında güvenli davranışları teşvik etmek ve bu alanda kariyer yapmayı düşünen öğrenciler için bir rehberlik sağlamaktır. İlk çalıştay, 17-18 Şubat 2018 tarihlerinde, ikincisi 18-20 Nisan 2018 ve 3. çalıştay 28-29 Kasım 2019 tarihlerinde gerçekleştirilmiştir. Katılımcılar arasında Cumhurbaşkanlığı İletişim Başkanlığı, Milli Eğitim Bakanlığı, çeşitli üniversiteler, İstanbul Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü ve birçok sivil toplum kuruluşu yer almıştır (İstanbul İl Milli Eğitim Müdürlüğü, 2018; Teknopark İstanbul MTAL, 2019).

- **Çalıştayların İçeriği ve Eğitim Programları**

Çalıştaylarda, siber güvenlik ve sosyal medya kullanımı konularında eğitim programları düzenlenmiş, çeşitli sunumlar ve atölye çalışmaları gerçekleştirilmiştir. Öğrencilerin ve öğretmenlerin siber güvenlik bilincini artırmak amacıyla CTF (Capture the Flag) yarışmaları düzenlenmiş, sosyal medya hesaplarının güvenliği, dijital ayak izi, siber zorbalık ve teknoloji bağımlılığı gibi konular ele alınmıştır. Ayrıca, öğrencilerin siber güvenlik alanında kariyer planlamalarına yardımcı olmak için çeşitli seminerler ve geziler organize edilmiştir (İstanbul İl Milli Eğitim Müdürlüğü, 2018). 3. çalıştayda ise siber güvenlik eğitiminin ortaöğretim düzeyinde kapsamlı bir şekilde verilmesinin gerekliliği, ilgili tüm paydaşlar tarafından vurgulanmıştır. Ayrıca, kurulması önerilen siber güvenlik lisesi veya ilgili teknik eğitim alanının geliştirilmesi için müfredatın hazırlanması ve bu müfredatın sürekli olarak güncellenmesi gerektiği de ifade edilmiştir. Çalışma gruplarınca bazı tavsiye politikalar, donanım, kadroların seçimi, öğrencilerin seçimi ve müfredat önerileri konularında çalışmalar yapılmıştır (Teknopark İstanbul MTAL, 2019). Bu 3 çalıştayın neticesinde aşağıda yer verilecek olan ülkemizdeki ilk siber güvenlik temalı ortaöğretim kuruluşunun temelleri atılmış ve hayata geçirilmiştir.

Tablo 33 *1. Çalıştay: 17-18 Şubat 2018 Tarihli Siber Güvenlik ve Sosyal Medyanın Doğru Kullanımı Çalıştayı Çalışma Grupları ve Konular (İstanbul İl Milli Eğitim Müdürlüğü, 2018, s.22)*

Çalışma Grupları	Konular
1. Grup	Sosyal Medyanın Doğru Kullanılması Bir Meslek Olarak Sosyal Medya Uzmanlığı Sosyal Medya Okuryazarlığı
2. Grup	Siber Zorbalık ve Teknoloji Bağımlılığı Kişisel Mahremiyetin Korunması Dijital Ayak İzi Siber Ahlak
3. Grup	Siber Güvenlik Farkındalığı Oluşturma ve Artırma
4. Grup	Temel Seviye Siber Güvenlik Önlemleri Kriterlerinin Oluşturulması
5. Grup	Bir Meslek Olarak Siber Güvenlik Uzmanlığı ve Eğitimleri

Tablo 34 *2. Çalıştay: 18-20 Nisan 2018 Tarihli Siber Güvenlik ve Sosyal Medyanın Doğru Kullanımı Çalıştayı: Program Yazma Süreci - Çalışma Grupları ve Ana Konular (İstanbul İl Milli Eğitim Müdürlüğü, 2018, s.60-61)*

Çalışma Grubu	Ana Konular
1. Çalışma Grubu	Bilinçli Sosyal Medya Kullanımı Temel Seviye Öğretmen Yetiştirme Standart Eğitim Programının Oluşturulması Pilot Uygulama İçin Program, Ders Planları ve Öğretim Yöntemlerinin Hazırlanması
2. Çalışma Grubu	Temel ve İleri Seviye Siber Güvenlik Öğretmen Yetiştirme Standart Eğitim Programının Oluşturulması Pilot Uygulama İçin Program, Ders Planları ve Öğretim Yöntemlerinin Hazırlanması

Not: Bu tablo, belirtilen kaynaktaki verilerin derlenmesiyle oluşturulmuştur.

Tablo 35 *3. Çalıştay: 28-29 Kasım 2019 Tarihli Siber Güvenlik ve Sosyal Medyanın Doğru Kullanımı Çalıştayı: Bir Meslek Alanı Olarak Siber Güvenlik - Çalışma Grupları ve Ana Konular (Teknopark İstanbul MTAL, 2019, s.16-43)*

Çalışma Grubu	Ana Konular
Aziz Sancar Çalışma Grubu	Lise'ye Öğrenci Kabul Koşulları Nasıl Olmalıdır?
	Lisede Okutulacak Dersler ve Öğretim Programı Nasıl Olmalıdır?
	İşletmelerde Mesleki Eğitim Durumu (Staj) Nasıl Olmalıdır?
	Okulun Fiziki Yapısı Nasıl Olmalıdır?
	Öğretmen ve Yönetici Seçme Kriterleri Nasıl Olmalıdır?
	Okul, Öğretmen ve Yönetici Gelişim Politikaları Neler Olmalıdır?
	Mezuniyet Sonrası Kariyer Planlaması Nasıl Olmalıdır?
Hezarfen Çalışma Grubu	Siber Güvenlik Lisesine Öğrenci Seçimi Nasıl Olmalıdır?
	İşletmelerde Siber Güvenlik Mesleki Eğitim Durumu (Staj) Nasıl Olmalıdır?
	Siber Güvenlik Lisesinin Fiziki Yapısı Nasıl Olmalıdır?
	- Öğretmen ve İdareci Seçme Kriterleri Neler Olmalıdır?
	- Siber Güvenlik Okullarının Öğretmen ve Yönetici Gelişim Politikaları Nasıl Olmalıdır?
	- Mezuniyet Sonrası Kariyer Planlanması, Mesleki ve Akademik Gelişim Nasıl Olmalıdır?
	- Lisede Okutulacak Dersler ve Öğretim Programları Nasıl Olmalıdır?
Cezeri Çalışma Grubu	- Siber Güvenlik Alanı/Okullarının Öğrenci Kabul Koşulları Nasıl Olmalıdır?
	- İşletmelerde Siber Güvenlik Mesleki Eğitim Durumu (Staj) Nasıl Olmalıdır?
	- Siber Güvenlik Liselerinin Fiziki Yapısı Nasıl Olmalıdır?
	- Bu Tür Okulların Öğretmen ve Yönetici Seçme Kriterleri Neler Olmalıdır?
	- Siber Güvenlik Liselerinin Öğretmen ve Yönetici Gelişim Politikaları Nasıl Olmalıdır?
	- Mezuniyet Sonrası Kariyer Planlaması Nasıl Olmalıdır?
Nuri Demirağ Çalışma Grubu	- Siber Güvenlik Liseleri ve Sosyal Medyanın Doğru Kullanımı Dersleri için Örnek Ders Planlarının Yazılması
	- 2023 Eğitim Vizyonu Kapsamında Siber Güvenlik ve Bilinçli Sosyal Medya Kullanımı Müfredatının Geliştirilmesi
	- Öğretmenlerin Standart Eğitim Programları, Çalıştay ve Seminerler ile Yetiştirilmesi
	- Program, Ders Planları ve Öğretim Yöntemlerinin Pilot Uygulamasının Yapılması

Not: Bu tablo, belirtilen kaynaktaki verilerin derlenmesiyle oluşturulmuştur.

- **Çalıştayların Sonuçları ve Etkileri**

Çalıştaylar sonucunda, siber güvenlik alanında farkındalığın arttığı, katılımcıların bu alandaki bilgi ve becerilerinin geliştiği gözlemlenmiştir. Özellikle öğretmenlerin bilinçlendirilmesi ve onların aracılığıyla öğrencilerin eğitilmesi, toplumsal güvenlik açısından önemli bir adım olmuştur. Çalıştaylar, gelecekte benzer etkinliklerin daha yaygın olarak düzenlenmesi gerektiğini ortaya koymuş ve siber güvenlik eğitiminin önemini bir kez daha vurgulamıştır. Daha da önemlisi bu çalışmaların neticesinde somut bir adım atılmış ve çalışmamızda da yer verilmiş olan Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi kurulmuş ve eğitim öğretime başlamıştır.

Tablo 36 Milli Eğitim Bakanlığı Uhdesinde 2018 – 2019 Yıllarında Düzenlenen Siber Güvenlik Konulu Çalıştaylar *(İstanbul İl Milli Eğitim Müdürlüğü, 2018; Teknopark İstanbul MTAL, 2019)*

Tarih	Çalıştay İsmi	Katılımcı Sayısı
17-18 Şubat 2018	Siber Güvenlik ve Sosyal Medyanın Doğru Kullanımı Çalıştayı	150
18-20 Nisan 2018	Siber Güvenlik ve Sosyal Medyanın Doğru Kullanımı: Program Yazma Süreci Çalıştayı	200
28-29 Kasım 2019	Bir Meslek Alanı Olarak Siber Güvenlik Çalıştayı	83 (*Sadece Çalışma Gruplarına Katılanların Sayısıdır*)

4.4.3.7.Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi (MTAL)

Türkiye'de siber güvenlik eğitimi politikası, ülkenin dijital dünyada güvenliğini sağlamak için kritik bir öneme sahiptir. Bu bağlamda, Milli Eğitim Bakanlığı'nın liderliğinde kurulan Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi, bu politikanın önemli bir ürünüdür. 2020 yılında faaliyete

geçen okul, siber güvenlik alanında nitelikli bireyler yetiştirmeyi hedeflemektedir (Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi, 2021).

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi, öğrencilerine bilişim teknolojileri ve siber güvenlik alanında kapsamlı bir eğitim sunmaktadır. Okulun modern eğitim altyapısı ve sektörel iş birlikleri, öğrencilerin bu alanda kariyer yapabilmeleri için gerekli bilgi ve becerileri kazanmalarını sağlamaktadır. İstanbul Üniversitesi-Cerrahpaşa ve Boğaziçi Üniversitesi gibi önemli akademik kurumlarla yapılan iş birlikleri, eğitimin kalitesini daha da artırmaktadır (Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi, 2021).

Milli Eğitim Bakanlığı'nın siber güvenlik eğitimi konusundaki bu girişimi, ülkemizin dijital güvenlik alanındaki rekabet gücünü artırmayı hedeflemektedir. Öğrenciler, çeşitli projeler ve uluslararası programlar aracılığıyla hem teorik hem de pratik bilgiye sahip olmaktadır. Özellikle European Region Action Scheme for the Mobility of University Students Plus (Avrupa Birliği Üniversite Öğrencilerinin Hareketliliği için Bölgesel Eylem Planı Artı - ERASMUS+) programı kapsamında geliştirilen bulut bilişim eğitim modülleri ve siber güvenlik hızlandırma ve kuluçka programları, bu alandaki yenilikçi yaklaşımların örneklerindendir.

Sonuç olarak, Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi, Türkiye'nin siber güvenlik eğitimi politikasının önemli bir parçasıdır. Okulun misyonu, bilgi güvenliği konusunda yetkin, girişimci bireyler yetiştirmektir. Bu tür okulların sayısının artması, ülkemizin dijital dünyada daha güvenli ve rekabetçi bir konuma gelmesine katkı sağlayacaktır (Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi, 2021).

Tablo 37 *Teknopark İstanbul MTAL Okul Öğrenci Sınıf , Şube ve Öğrenci Sayıları* (*Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi, 2021)*

Öğrenci Sayısı	Sınıf	Şube Sayısı
30	Hazırlık	2
30	9. Sınıf	2

4.4.3.8.Baykar Milli Teknoloji Mesleki ve Teknik Anadolu Lisesi

Baykar Milli Mesleki ve Teknik Anadolu Lisesi (MTAL), 31 Mayıs 2023 tarihinde faaliyete geçen bir proje okuludur. Bu okul, Bilişim Teknolojileri ve Havacılık ve Uzay Teknolojisi olmak üzere iki ana eğitim alanında dersler sunmaktadır. Milli ve manevi değerlerle donatılmış, ülkesinin bağımsızlığını ve özgürlüğünü koruma bilincine sahip bireyler yetiştirmeyi hedeflemektedir (Baykar Milli MTAL, 2024a; Baykar Milli MTAL, 2024b).

Baykar Milli MTAL, müfredatında Siber Güvenlik Temelleri Dersi'ne yer verir. Bu dersin amacı, öğrencilere siber güvenlik alanında gerekli temel bilgi ve becerileri kazandırmaktır (Baykar Milli MTAL, 2024a; Baykar Milli MTAL, 2024b).

Siber Güvenlik Temelleri Dersi, öğrencilere şu konularda eğitim sunar:

- Siber Güvenliğe Giriş
- Bilgi Toplama Teknikleri
- Sızma Testi Teknikleri
- Sniffing Yöntem ve Uygulamaları
- Şifreleme Teknikleri
- Parola Atakları
- DoS ve DDoS Atakları
- SQL ve Man in The Middle Atakları
- Kablosuz Ağ Güvenliği
- Web Güvenliği (Baykar Milli MTAL, 2024a; Baykar Milli MTAL, 2024b).

Bu ders ayrıca öğrencilere, siber güvenlik dünyasındaki güncel tehditler, güvenlik önlemleri ve etik hackerlık konularında detaylı bilgi sağlar. Öğrenciler, bu sayede teorik bilgilerini pratiğe dökerek siber güvenlik alanında yetkinlik kazanırlar (Baykar Milli MTAL, 2024a).

Baykar MTAL'nin siber güvenlik programı, öğrencilere teknik beceriler kazandırmanın ötesinde, etik hackerlık prensiplerini de öğretir. Bu sayede öğrenciler, siber güvenlik alanında sorumlu ve etik kurallar çerçevesinde

hareket edebilecek bilgi ve becerilere sahip olurlar (Baykar Milli MTAL, 2024b).

4.5.TÜRKİYE'DE SİBER TEHDİTLER VE SAVUNMA MEKANİZMALARI

Siber tehditler, ulusal güvenlik açısından ciddi riskler oluşturmaktadır. Dijitalleşmenin hızla yaygınlaşmasıyla birlikte Türkiye, bu tehditlere karşı çeşitli savunma mekanizmaları geliştirerek ulusal güvenliğini koruma çabasındadır. Siber saldırılar, bireyler, devlet kurumları, kritik altyapılar ve özel sektör üzerinde büyük bir tehdit oluşturmaktadır (Ülgen et al., 2015).

Türkiye'de siber güvenlik politikaları, ulusal güvenliği sağlamak için stratejiler ve önlemler içermektedir. Bu stratejiler arasında siber tehdit istihbaratının toplanması, bilgi güvenliği mimarisinin oluşturulması ve acil durum müdahale ekiplerinin kurulması yer alır (Halisdemir, 2021). Ayrıca, özel sektör ve kamu kurumları arasında iş birliği sağlanarak daha etkili bir savunma mekanizması oluşturulmaktadır (Ülgen ve ark., 2015).

Siber tehditler, kritik altyapılara yönelik saldırılar, siber casusluk, fidye yazılımları ve DDoS saldırıları gibi çeşitli biçimlerde ortaya çıkabilir. Türkiye, bu tehditlere karşı proaktif savunma mekanizmalarını geliştirerek sürekli güncellenen güvenlik yazılımları, saldırı tespit ve önleme sistemleri, güvenlik duvarları ve düzenli güvenlik denetimleri gibi önlemler almaktadır (Ülgen ve ark., 2015).

4.5.1. Türkiye'de Siber Tehditler ve Savunma Stratejileri

Türkiye, kritik altyapılara yönelik saldırılar, siber casusluk, fidye yazılımları ve DDoS saldırılarına karşı savunma stratejileri geliştirmiştir. Bu stratejiler, güvenlik yazılımları, saldırı tespit ve önleme sistemleri (IDS/IPS), güvenlik denetimleri ve personel eğitimi gibi unsurları içermektedir. Bu mekanizmalar, siber tehditlerin hızlı tespit edilip etkisiz hale getirilmesini sağlamaktadır (Liszkowska, 2024).

Türkiye ayrıca, ulusal ve uluslararası iş birlikleri yaparak, siber tehditlere karşı ortak savunma stratejileri geliştirmektedir. NATO ve Avrupa Birliği gibi kuruluşlarla yapılan iş birlikleri, Türkiye'nin siber tehditlere karşı daha güçlü

bir savunma sağlamasına yardımcı olmaktadır (Halisdemir, 2021). Siber tehditlere karşı alınan önlemler arasında bilgi güvenliği standartlarının belirlenmesi ve uygulanması da önemli yer tutmaktadır. Türkiye'de bilgi güvenliği politikaları, veri koruma, erişim kontrolü, ağ güvenliği ve güvenlik denetimleri gibi unsurları kapsamaktadır (Özker, 2022).

4.5.2. Türkiye'nin Siber Savunma Mekanizmaları ve Önlemleri

Türkiye, sürekli güncellenen güvenlik yazılımları, saldırı tespit ve önleme sistemleri, düzenli güvenlik denetimleri ve personel eğitimi gibi savunma mekanizmaları geliştirmiştir. Ayrıca, siber tehditlerin hızlı tespit edilerek etkisiz hale getirilmesi amacıyla acil müdahale ekipleri kurulmuştur. Bu ekipler, siber saldırıların ardından hasarı en aza indirerek sistemlerin en kısa sürede normale dönmesini sağlamaktadır (Halisdemir, 2021).

Siber güvenlik alanında ulusal ve uluslararası iş birlikleri, Türkiye'nin siber tehditlere karşı dirençli bir savunma oluşturmasına katkı sağlamaktadır. Türkiye, NATO ve AB gibi kuruluşlarla bilgi paylaşımı yaparak, siber güvenlik kapasitesini artırmaktadır. Ayrıca, uluslararası standartlar ve politikalarla uyumlu güvenlik politikaları geliştirilmektedir (Eitan, 2018).

4.5.3. Özel Sektör ve Kamu Kurumları İş Birliği ile Siber Güvenlik

Özel sektör ve kamu kurumları arasındaki iş birliği, Türkiye'nin siber tehditlere karşı etkili savunma stratejileri geliştirmesini sağlamaktadır. Bilgi paylaşımı, ortak projeler ve eğitim programları gibi iş birlikleri, siber tehditlere karşı inovatif çözümler üretilmesine katkıda bulunmaktadır. Türkiye, bu iş birlikleri sayesinde siber güvenlik alanında önemli ilerlemeler kaydetmektedir (Trade.gov, 2024).

Türkiye, uluslararası düzeyde de çeşitli iş birlikleri yaparak siber güvenlik kapasitesini artırmaktadır. AB ve NATO gibi çok uluslu kuruluşlarla iş birliği yaparak, ortak savunma stratejileri geliştirmekte ve siber güvenlik farkındalığını artırmak amacıyla eğitim programları ve tatbikatlar düzenlemektedir (EC-Council, 2024).

4.5.4. Ulusal ve Uluslararası İş Birlikleri

Siber güvenlik alanında ulusal ve uluslararası iş birlikleri, siber tehditlere karşı güçlü bir savunma oluşturmanın anahtarıdır. Türkiye, hem ulusal düzeyde kamu ve özel sektörle iş birlikleri yapmakta hem de uluslararası kuruluşlarla ortak çalışmalarda bulunmaktadır. Bu iş birlikleri, bilgi paylaşımı, ortak projeler, eğitim ve politika geliştirme gibi birçok alanı kapsamaktadır.

Bölgesel iş birlikleri ve ikili anlaşmalar, Türkiye'nin siber güvenlik stratejilerinin önemli bir parçasını oluşturmaktadır. Türkiye, bölgesel düzeyde Balkanlar, Orta Doğu ve Kafkasya gibi bölgelerdeki ülkelerle iş birlikleri yaparak siber tehditlere karşı ortak savunma stratejileri geliştirmektedir (Halisdemir, 2021).

Uluslararası eğitim ve tatbikatlarla Türkiye, siber güvenlik kapasitelerini artırmakta ve uluslararası politika geliştirme süreçlerine katılmaktadır. Bu süreçler, Türkiye'nin siber güvenlik politikalarını geliştirmesine ve uluslararası standartlara uyum sağlamasına yardımcı olmaktadır (EC-Council, 2024).

4.6.TÜRKİYE'DE SİBER GÜVENLİK EKOSİSTEMİ

Siber güvenlik, Türkiye'de stratejik bir öneme sahiptir ve ülkenin dijital altyapısını korumak için özel sektör, devlet kuruluşları, üniversiteler ve STK'lar arasında geniş bir iş birliği gerektirmektedir. Bu bölümde, Türkiye'nin siber güvenlik ekosistemini oluşturan ana bileşenler ve bu ekosistemin etkinliği üzerine detaylı bir inceleme yapılacaktır. Türkiye'nin siber güvenlik politikalarının güçlü bir şekilde hayata geçirilmesi ve sürekli güncellenmesi, ulusal güvenlik açısından büyük önem taşımaktadır (Lexology GTDT, 2022).

4.6.1. Türkiye'de Siber Güvenlik Ekosistemi'nde Mevcut Durum

Siber güvenlik ekosistemi, içerisinde çeşitli aktörlerin yer aldığı çok katmanlı bir yapıya sahiptir. Devletin regülatif ve yasal çerçeveleri, özel sektörün teknolojik gelişmelere yanıt verme kapasitesi, akademik kurumların araştırma ve geliştirme faaliyetleri ve sivil toplum kuruluşlarının farkındalık yaratma çalışmaları, bu ekosistemin temel taşlarını oluşturur. Bu çeşitlilik, Türkiye'nin siber güvenlik stratejilerinin kapsamlı ve dinamik olmasını sağlamaktadır (ISPI, 2022; Beghe Sönmez & Karakaşlar, 2023).

4.6.2. Türkiye'de Siber Güvenlik Ekosistemi'nde Gelecek Perspektifleri

Türkiye'nin siber güvenlik ekosisteminin gelecekte daha da güçlenmesi için çeşitli stratejik adımlar atılması gerekmektedir. Öncelikle, devlet kurumları, özel sektör ve akademik kurumlar arasındaki iş birliğinin artırılması, siber güvenlik alanında daha etkili çözümler üretilmesini sağlayacaktır. Ayrıca, siber güvenlik alanındaki yasal düzenlemelerin güncellenmesi ve uluslararası standartlara uyum sağlanması önemlidir.

Gelecekte, siber güvenlik eğitiminin yaygınlaştırılması ve bu alanda uzmanlaşmış bireylerin yetiştirilmesi, Türkiye'nin siber tehditlere karşı daha dirençli olmasını sağlayacaktır. Bunula birlikte, siber güvenlik alanında yapılan araştırma ve geliştirme faaliyetlerinin artırılması, yeni tehditlere karşı yenilikçi çözümler geliştirilmesine olanak tanıyacaktır (ISPI, 2022).

Türkiye'nin siber güvenlik ekosisteminin gelecekteki başarısı, bu alandaki paydaşların birlikte çalışması ve sürekli gelişim göstermesi ile mümkün olacaktır ve böylelikle siber güvenlik stratejilerinin ve politikalarının dinamik ve esnek olması, yeni tehditlere hızla adapte olabilme yeteneğini artıracaktır.

5. SONUÇ

Siber uzayda en önemli strateji alanlarından birisi haline gelen sosyal medyada Türkiye'de ilk ciddi hareketlenme 27 Mayıs 2013'de alevlenen Gezi Parkı olaylarıyla başlayan süreçte yaşanmıştır. Arap baharında özellikle Mısır'da yaşananlara benzer bir tablo oluşturulmaya çalışılan sosyal medyada manipülasyonlar ve örgütlenmeler birbirine karışmış ve Türkiye çok sıkıntılı bir süreç yaşamıştır. İkinci önemli sosyal medya hareketi ise; 17-25 Aralık diye tabir edilen süreçte yaşanmıştır. Uluslararası kaynaklardan sosyal medya ortamına aktarılan ve çok kritik yöneticilere ve onların ailelerine ait, özel ve mali ilişkilerine yönelik, orijinalliği ve montajlanmış olması tartışmaları hala devam etmekte olan onlarca sesli ve görüntülü kaydın servis edildiği sıkıntılı ve etkileri hala devam eden bir sürecin içine girmiştir. Kabineden dört bakanın istifasıyla sonuçlanan bu süreç, siyasi anlamda çokça tartışılmaktadır ancak işin siber uzaydaki boyutunun analizi ve tespiti ciddi bir eksiklik olarak önümüzde durmaktadır. Seçim sürecinde de katlanan ve sınırları zorlayan sosyal medya hareketleri, halkta ciddi bir gerginliğe yol açmaktadır. Özellikle bilişim eğitiminin çok eksik kaldığı değerlendirilen ülkemizin gençleri açısından bu süreç, siber espiyonaj faaliyetleri açısından ve siber uzaydaki kısıtlamaları aşmak adına kullanılan yöntemlerin milyonlarca bilgisayarı ilerdeki olası bir siber savaşta gizli silah durumuna sokabilecek riskler taşıdığından ulusal güvenliğimiz açısından ciddi bir şekilde araştırılması ve önlem alınması gereken toplumsal ve teknolojik bir vaka durumundadır. Yukarda saydığımız hareketlenmelerin akabinde gerçekleşen 3.'sü ise siber uzayın ülkemiz açısından belki de en önemli gelişmesi 15 Temmuz 2016 hain darbe girişimi gecesinde yaşanmıştır. 12 Eylül 1980'den sonra 36 yılın en sıcak, en acı ve bir o kadar da halkın canını ortaya koyan onurlu feraseti ile milyonların uykusuz ve hatta mücadele içerisinde geçirdiği saatlerde; ülkemizin darbeler tarihinde radyo ve televizyon ekranlarıyla sınırlı kalan ve kontrol altında tutulması nispeten çok kolay olan kitle iletişimi; siber uzay ve siber uzayın en önemli unsurlarından olan sosyal medya sayesinde halk iradesine kast edenlerin propaganda stratejilerine en büyük keti vurarak halkın bu kalkışmaya karşı organize olarak engel olmasını sağlamıştır.

İnsanların yaşadıkları her ortamda var olan diplomasi de bu yeni alanda hızla yayılmaktadır. Bu yeni soyut alanın sonsuz imkânlarıyla şekillenen yeni bir diplomasi anlayışıyla ve yeni diplomasinin siber uzayın imkânlarıyla zihinlerde çok daha düşük maliyetlerle yüksek etki bırakabilecek uygulamalarının hızla yayılmasıyla son derece etkili bir hareket alanı kazanmaktadır.

Günümüzde karasal ve dijital TV yayınlarının ulaştığı 18 milyon hanenin reklam gelirlerinin 2,5 milyar doları aştığı bilgisini bir kenarda tutup artık 80 milyonu aşan nüfusumuza alt yapı maliyeti çok daha düşük olanaklarla hatta son dönemde mobil cihazların da yaygınlaşmasıyla bu sayının git gide arttığı ve her yerden ulaşım imkânıyla yukarıda verdiğimiz reklam gelirlerinin siber uzayda onlarca katına ulaşıldığını göz ardı etmemek gerekir. Yukarıdaki veri vergilendirilebilir hesap verebilir kurumlar olan yayın şirketlerinin kayıtlarından elde edebilmekteyken bugün sosyal medyanın denetimden uzak, yetersiz hukuki düzenlemeler ve uluslararası hukuktan çıkarlarına kullanabildikleri, tutunabildikleri maddeler sayesinde toplumun bu konuda manipüle edilerek konunun erişim özgürlüğü platformuna çekilmektedir. Böylece Facebook, Twitter, Instagram, Youtube gibi başı çeken sosyal medya ortamlarının bilgi toplumunun zoraki tüketicisi konumunda olan halkın üzerinden hem milyarlarca doları vergisiz kazanabilmelerine, hem de sosyal medyanın kitleleri harekete geçirebilme gücünü ellerinde bulundurmaları dolayısıyla devletler üstü bir yumuşak güç maliki konumuna gelmelerine imkân tanımaktadır. Bu yeni durum bir bakıma kamu diplomasisinin en önemli unsurlarından biri konumuna gelmiş şekilde değerlendirilebileceği gibi bir başka ifadeyle diplomasinin siber uzaydaki hali olarak kısaca tanımlanabilecek yeni bir diplomasinin; "*siber diplomasi*"'nin önemli bir kurum olarak tesisini de kaçınılmaz kılmaktadır.

Soğuk savaş esnasında özellikle iletişim teknolojilerindeki gelişmeler ve uzay yarışı esnasında ABD ve Rusya'nın farkına vararak önlem almaya çalıştığı ve karşı atak için hazırlıklar yaptığı bilinmektedir. 80'li yıllarda Hollywood *"War Games"* adlı yapımla 30 yıl önceden siber savaşın olasılığını ve ciddiyetini ortaya koymuşken Türkiye'nin daha bu konuda stratejisini son birkaç yılda geliştirmekte olduğu gerçeği çok büyük bir eksikliktir. Ancak son yıllarda atılan adımlar en azından geleceğe yönelik ülkemizin kendi savunma gücünü

ve stratejisini oluşturmakta olduğunu göstermesi açısından önemlidir. Bu konu Türkiye ile sınırlı kalmamalı, Ortadoğu ile yakından ilgilenen bir ülke olarak bölgedeki kardeş ülkelerin gerek eğitim gerek ise alt yapı açısından Türkiye ile birlikte gelişmeleri ve ortak hareket kabiliyetleri kazanılabilmesi için desteklenmesi gereği aynı zamanda Türkiye'nin de siber uzaydaki güvenliği açısından önem taşımakta olduğu bilinciyle hareket edilmelidir. Çünkü siber uzayda coğrafi sınırlardan bahsetmek mümkün değildir, siber uzayda eğer bir çevreleme ya da savunma yapılacaksa, bunda dünyanın birbirine en uzak 2 ülkesinin dahi komşu konumunda olduğunu unutmamak gerekir. Aynı şekilde sosyal medya ve sosyal medyadaki büyük veri kaynağının istihbari açıdan önemi ve ülkelerin temellerini sarsacak nitelikte olması bu konuda sansür yaftasından kurtulacak şekilde, ulusal güvenlik politikaları çerçevesinde, uluslararası hukuka uygun olarak egemenlik haklarımız gözetilerek insanlarımızın gönüllü dahi olsa verilerini savurganca paylaşıyor olmalarını azaltacak ve idealde önleyecek tedbirlerin acilen alınması gerekmektedir. Asırlardır hep kaynamakta olan coğrafyamızın altındaki ateşi körüklemekte en etkili yöntem haline gelen sosyal mühendisliğe; karşı mühendislik faaliyetleriyle karşılık verilmeli, stratejiler geliştirilmelidir.

Siber güvenlik politikalarının geliştirilmesi ve uygulanması, dijital çağın vazgeçilmez bir gerekliliği haline gelmiştir. Türkiye'nin bu alandaki politikaları, hem ulusal güvenliği sağlamaya yönelik adımları hem de eğitim yoluyla siber güvenlik bilincini artırma çabalarını kapsamaktadır. Bu çalışmada, siber güvenlik politikalarının eğitimle desteklenmesi ve Türkiye'nin bu alandaki eğitim politikaları detaylıca ele alınmış ve özellikle siber uzayda bireylerin siber güvenlik konusundaki eğitimlerinin bu doğrultudaki en önemli unsurlardan birisi olduğu vurgulanmıştır.

Türkiye, siber güvenlik politikalarını ulusal güvenlik stratejisinin önemli bir parçası olarak görmekte ve bunların etkin bir şekilde uygulanması adına çeşitli adımlar atmaktadır. Bunlardan resmî olarak atılmış olan en önemli adım 20/10/2012 tarihli ve 28447 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren kararla Siber Güvenlik Kurulu oluşturulması kararıdır. Bu kurulun çalışmaları neticesinde 2013 yılında oluşturulan "Ulusal Siber Güvenlik Stratejisi" ile bu stratejiye bağlı eylem planları, Türkiye'nin siber güvenlik

alanındaki kararlılığını ve bu konudaki ciddi yaklaşımını göstermektedir. Bu stratejik belgeler, yasal düzenlemeler, adli süreçlerin desteklenmesi, ulusal siber olaylara müdahale organizasyonunun kurulması ve nitelikli insan kaynağının yetiştirilmesi gibi önemli bileşenleri içermektedir.

Ancak, yapılan çalışmalar göstermektedir ki; Türkiye'de siber güvenlik eğitimine yönelik farkındalık ve eğitim programları henüz istenen seviyeye ulaşamamıştır. Özellikle okullarda ve üniversitelerde siber güvenlik eğitiminin müfredatlara entegre edilmesi gerekmektedir. Bu noktada, ulusal ve uluslararası iş birliklerinin, siber güvenlik eğitiminde önemli bir rol oynadığı açıkça görülmektedir ve bu konuda teşvik ve yönlendirmelerin kamu yönetimi açısından daha fazla üzerinde durulması gereken hususlar olduğu değerlendirilmektedir.

Siber güvenlik alanının sosyal bilimler ve fen bilimleri alanlarının her biriyle olan güçlü ilişkisi bu alanda yapılan çalışmaların aslında bu iki alan açısından hangi pencereden bakılırsa diğeri açısından zayıf kalmasının kaçınılmazlığını ortaya koymaktadır.

ABD, Çin, Hindistan, Avustralya ve Rusya gibi ülkeler, siber güvenlik eğitimine büyük önem vermektedir. Bu ülkeler, ulusal güvenlik stratejilerinin bir öğesi olan siber güvenlik eğitim programlarını hayata geçirmekte ve sürekli olarak güncellemektedirler. Örneğin, ABD'nin Ulusal Siber Güvenlik Eğitimi İnisiyatifi (NICE) ve CyberCorps® gibi programları, ülke genelinde siber güvenlik farkındalığını artırmak ve bu alanda uzmanlaşmış bir iş gücü yetiştirmek amacıyla tasarlanmıştır. Çin, siber güvenlik eğitimini ilkokullardan üniversitelere kadar geniş bir yelpazede uygulamaktadır. 2017 yılında yürürlüğe sokulan Siber Güvenlik Yasası, eğitim kurumlarının siber güvenlik farkındalığını artırmalarını zorunlu kılmaktadır. Bu kapsamda Çin hükümeti, siber güvenlik araştırma ve geliştirmelerine büyük yatırımlar yapmaktadır

Türkiye'nin siber güvenlik eğitim politikaları, diğer ülkelerle karşılaştırıldığında henüz gelişim aşamasındadır. Hatta çalışmamızın sonucunda görülmüştür ki henüz siber güvenlik politikalarındaki gelişimin eğitim özelinde odaklandığı ve ela alındığı ciddi bir siber güvenlik eğitimi politikası geliştirme süreçlerine henüz geçilememiştir. Bu açıdan çalışmamızın

bu eksikliğe ışık tutması ve bu konuda adımların hızlandırılmasına vesile olması umulmaktadır. Siber Güvenlik Kurulu ve akabindeki Ulusal Siber Güvenlik Stratejisi ile bu stratejiye bağlı eylem planları, siber güvenlik eğitimine yönelik önemli bazı adımları içerse de, bu alanda daha kapsamlı ve süreklilik arz edecek tarzda bir eğitim sistemine ihtiyaç vardır. Türkiye'nin siber güvenlik eğitiminde başarısı, eğitim müfredatlarının güncellenmesi, öğretmenlerin bu alanda eğitilmesi ve öğrencilerin siber güvenlik konularında bilinçlendirilmesi ile mümkün olacaktır. Siber güvenlik eğitiminde atılması gereken adımlar, teorik ve pratik uygulamaları da mutlaka içermelidir. Siber saldırı simülasyonları, güvenli internet kullanımı eğitimleri ve şifre yönetimi gibi konular, siber güvenlik eğitim programlarının önemli bileşenleri olmalıdır.

Sonuç olarak, siber güvenlik politikalarının tesirli ve sonuç alınabilecek şekilde uygulanabilmesi adına eğitim ve daha da önemlisi eğitimin bireyler tarafından içselleştirilmesini sağlayabilecek bir farkındalık ve kazanımlar bütünüyle bireyi donatabilecek bir eğitim politikasının uygulanabilmesi en önemli öğelerden biridir. Türkiye, siber güvenlik alanında ulusal ve çok uluslu iş birliklerini artırmalı, eğitim müfredatlarını güncellemeli ve toplum genelinde siber güvenlik bilincini yaygınlaştırmalıdır. Söz konusu hedeflere ulaşmak adına, diğer ülkelerin başarılı uygulamalarından yararlanılabilir ve Türkiye'nin hazırbulunuşluk ve yerel dinamikleri çerçevesinde özgün ihtiyaçlarına uygun stratejiler geliştirilmelidir.

Çalışma neticesinde bazı politika ve uygulama önerileri aşağıda ifade edilmeye çalışılmıştır:

- **Ebeveyn Eğitimleri:** Bu madde eklenirken bunun toplumsal birçok sorunda aslında ihmal edildiği değerlendirilmekte olsa da bunlar umulur ki başkaca çalışmaların konuları olacaktır. Bu çalışma açısından bakıldığında, eğitimin temelleri ailede atılmaktadır dolayısıyla ailede siber güvenlik temel bilinci ve hassasiyetleri açısından doğru temellerin atılması kritik önemdedir. Yuva kuracak ebeveyn adaylarından mevzuatta aranan şartlar arasında bazı kritik sağlık testleri dışında bir yeterlik özellikle de eğitim koşulu yer almamaktadır. Oysaki bir makinenin kullanılmasında dahi eğitimler, sınavlar sonucu alınması gereken bir sertifika ya da ehliyet söz konusuyken, toplumun

geleceğinin mimarı olacak nesilleri dünyaya getirmeye ve yetiştirmeye namzet kişilere bir makine operatörlüğü ya da otomobil kullanıcılığında olduğu kadar dahi kriterler uygulanmamaktadır. Bu noksanlıktan hareketle, ebeveyn adaylarına evlilik öncesi birçok alanda uygulanacak bir eğitim ve sertifikasyon programının planlanması ve bu program içerisinde siber güvenlik konusuna da yer verilmesi önerilmektedir. Böylece ebeveyn adaylarının çocuk sahibi olduklarında aile içi eğitimlerimn programında yer alacak diğer ciddi konularla birlikte mutlaka bulunması gereken siber güvenlik konusunda da çok daha etkili olabilecekleri ve okul öncesi eğitime daha etkin bir hazırlayıcı rol oynayabilecekleri değerlendirilmektedir.

- **Aile İçi Eğitim:** Kuşkusuz her birey için eğitimin ilk ocağı olan aile siber güvenlik hususunda da tartışmasız en önemli ortamlardandır. Yukardaki maddede önerilen ebeveyn eğitimlerinin akabinde aile içi eğitimler için de Milli Eğitim Bakanlığı, Aile ve Sosyal Politikalar Bakanlığı, İçişleri Bakanlığı, Milli İstihbarat Teşkilatı (MİT), Yerel Yönetimler, Diyanet İşleri Başkanlığı, Radyo ve Televizyon Üst Kurulu (RTÜK) gibi kurumların da içinde yer alabileceği planlamalarla bu eğitimler çok daha zengin içeriklerle ve etkinliklerle desteklenebilir.
- **Eğitim Müfredatlarının Güncellenmesi:** Okullarda ve üniversitelerde siber güvenlik konularının müfredata dâhil edilmesi, öğrencilere erken yaşta siber güvenlik bilinci kazandıracaktır. Burda formal eğitimde erken yaştan kastedilen okul öncesi eğitimden başlayan farkındalık eğitimlerinin önemine dikkat çekmektedir. Ailede ebeveynlerce temelleri atılan bu farkındalıkların kalıcı öğrenmelere ve olumlu alışkanlıklara dönüştürülmesi okul öncesi eğitimlerde bu konuda hizmetiçi eğitimlerle hatta eğitim fakületelerindeki temel bilişim teknolojileri eğitimlerinin müfredatlarına eklenecek siber güvenlik konuları sayesinde okul öncesi öğretmenlerince etkili şekilde kazandırılabilir. Bu bağlamda, eğitim müfredatlarının güncellenmesi ve siber güvenlik konularının okul öncesinden üniversitelere kadar tüm eğitim katmanlarında ders programlarına stratejik bir perspektifte aşamalandırılarak dahil edilmesi gerekmektedir. ABD'nin NICE

inisiyatifi, okullarda siber güvenlik bilincini artırmak için geliştirilmiş kapsamlı bir modeldir. Türkiye de benzer şekilde, müfredatlarını güncelleyerek siber güvenlik eğitimini yukarda da bahsedildiği şekilde ailede başlayarak, okul öncesi eğitimden, ilkokuldan, ortaokuldan, liseden üniversite seviyesine kadar her basamakta yaygınlaştırmalıdır. Bu sayede, genç nesillerin siber tehditler karşısında daha uyanık ve hazırlıklı olmaları sağlanacaktır.

- **Öğretmen Eğitimi:** Siber güvenlik konusunda öğretmenlerin eğitilmesi, bu alandaki bilgi ve becerilerin öğrencilere kalıcı öğrenme oluşturacak şekilde ve tabii ki en doğru biçimde aktarılmasını sağlayacaktır. Öğretmenlerin siber güvenlik konusundaki bilgi düzeyinin artırılması, öğrencilerin bu alanda daha bilinçli bireyler olarak yetişmelerine katkıda bulunacaktır. ABD ve Avrupa'da uygulanan öğretmen eğitim programları, öğretmenlerin siber güvenlik konusunda donanımlı hale gelmesini sağlamakta ve bu bilgileri öğrencilere aktarmalarına yardımcı olmaktadır Türkiye'de de benzer öğretmen eğitim programları oluşturulmalı ve öğretmenlerin siber güvenlik konusunda sürekli olarak güncel bilgilerle donatılması sağlanmalıdır. Yukardaki maddede önerilen eğitim fakültelerinin müfredatlarında bulunan temel bilişim teknolojileri eğitimi kapsamında ya da müstakil bir siber güvenlik dersi şeklinde de organize edilebilecek bir güncellemeye acilen gerek duyulmaktadır.
- **Farkındalık Kampanyaları:** Toplum çapında siber güvenlik bilincini artırmak için düzenli kampanyalar ve etkinlikler düzenlenmelidir. Siber güvenlik bilincinin sadece okullarda değil, toplumun genelinde yaygınlaştırılması büyük önem taşımaktadır. Çin ve Hindistan gibi ülkeler, toplumsal çapta siber güvenlik bilincini artırmak için çeşitli kampanyalar ve etkinlikler düzenlemektedir. Türkiye'de de benzer kampanyalar düzenlenmeli ve halkın siber tehditler konusunda bilinçlenmesi sağlanmalıdır. Bu kampanyalar, sosyal medya, televizyon ve radyo gibi çeşitli iletişim kanalları kullanılarak geniş kitlelere ulaşmalıdır. Siber güvenlik eğitiminde farkındalık ve bilinçlendirme çalışmaları, bireylerin siber tehditlere karşı bilinçlenmesini ve bu

tehditlere karşı etkin savunma stratejileri geliştirmesini sağlar. Kamu ve özel sektör iş birliği ile düzenlenen farkındalık kampanyaları, bireylerin siber tehditler hakkında bilgi sahibi olmalarını ve çevrimiçi ortamda doğru ve güvenli davranışlar sergilemelerini teşvik etmektedir. Farkındalık ve bilinçlendirme çalışmaları, siber güvenlik eğitiminde önemli bir rol oynamaktadır. Kamu ve özel sektör iş birliği ile düzenlenen farkındalık kampanyaları, bireylerin siber tehditler hakkında bilgi sahibi olmalarını ve çevrimiçi ortamda doğru ve güvenli davranışlar sergilemelerini teşvik etmektedir. Bu kampanyalar, siber tehditlere karşı korunma bilincinin artırılmasına katkı sağlamakta ve bireylerin siber güvenlik konularında daha bilinçli hale gelmesini sağlamaktadır.

- **Uluslararası İşbirlikleri:** Diğer ülkelerle siber güvenlik eğitiminde iş birlikleri artırılmalı ve iyi uygulama örnekleri Türkiye'ye adapte edilmelidir. Uluslararası iş birlikleri, siber güvenlik eğitiminde bilgi ve deneyim paylaşımını kolaylaştırmakta ve küresel tehditlere karşı ortak stratejiler geliştirilmesini sağlamaktadır. ABD, AB ve NATO gibi çok uluslu kuruluşlar, siber güvenlik eğitiminde iş birliklerini teşvik eden önemli platformlardır Türkiye, bu tür uluslararası iş birliklerine katılarak siber güvenlik eğitiminde en iyi uygulama örneklerinden yararlanabilir ve kendi eğitim politikalarını geliştirebilir. Siber güvenlik eğitimi, ulusal ve uluslararası iş birlikleri ile güçlendirilebilir. Türkiye'deki üniversiteler ve araştırma merkezleri, uluslararası siber güvenlik eğitim programlarına katılarak, bu alandaki en iyi uygulamaları takip edebilir ve kendi eğitim programlarını geliştirebilir. Ayrıca, ulusal düzeyde gerçekleştirilen iş birlikleri, siber güvenlik eğitimine daha fazla kaynak sağlanmasını ve bu alandaki eğitimlerin etkinliğinin artırılmasını sağlayabilir. Ulusal ve uluslararası iş birlikleri, siber güvenlik eğitiminde önemli bir rol oynamaktadır. Türkiye'deki üniversiteler ve araştırma merkezleri, uluslararası siber güvenlik eğitim programlarına katılarak, bu alandaki en iyi uygulamaları takip edebilir ve kendi eğitim programlarını geliştirebilir. Ayrıca, ulusal düzeyde gerçekleştirilen iş birlikleri, siber güvenlik eğitimine daha fazla kaynak

sağlanmasını ve bu alandaki eğitimlerin etkinliğinin artırılmasını sağlayabilir

- **Pratik Eğitim Programları:** Siber saldırı simülasyonları, şifre ve parola yönetimi ve güvenli internet kullanımı gibi pratik eğitim programları düzenlenmelidir. Teorik bilginin yanı sıra, pratik uygulamaların da eğitim programlarına dahil edilmesi, öğrencilerin siber güvenlik konusunda daha donanımlı hale gelmelerini sağlayacaktır. ABD ve Avrupa'da düzenlenen siber saldırı simülasyonları ve pratik eğitim programları, öğrencilerin gerçek dünya senaryolarında deneyim kazanmalarını sağlamaktadır Türkiye'de de benzer programlar düzenlenmeli ve öğrencilerin siber güvenlik konusunda pratik beceriler kazanmaları sağlanmalıdır Bu çalışmanın literatüre katkısı, siber güvenlik politikalarının eğitimle desteklenmesi gerektiğini ve en önemlisi de siber güvenlik alanında bireylerin eğitiminin ve temel farkındalığın doğru ve etkili siber güvenlik eğitimi politikalarının geliştirilmesi ile sağlanabileceğini vurgulaması ve Türkiye'nin bu alandaki eksikliklerini ortaya koyarak öneriler sunmasıdır.

- **Kamu Kurumlarında Eğitim, Farkındalık ve Güvenlik Odaklı Siber Uzay Faaliyetleri Daire Başkanlığı Teşkilatlarının Kurulması**

Siber tehditlerin artan karmaşıklığı ve ölçeği, özellikle kamu kurumlarında siber güvenlik için stratejik ve organize bir yaklaşımı zorunlu kılmaktadır. 2012 yılında kurulan Siber Güvenlik Kurulu'nun etkili ve süreçte aktif olarak politikalara ve uygulamalara eşzamanlı ve ani müdahalelerinin mümkün olamadığı zaten kuruluş şeklinde de bir üst danışma istişare kurulu şeklinde kurulmuş olmasının da etkisi vardır ve ne yazık ki bu kurulun yeterli sıklıkta toplanmadığı görülmektedir. Bu tezin bulguları doğrultusunda, Türkiye'de kamu kurumları bünyesinde "Eğitim, Farkındalık ve Güvenlik Odaklı Siber Uzay Faaliyetleri Daire Başkanlıkları" 'nın kurulması önerilmektedir. Siber Güvenlik Kurulu'nun koordinasyonunda siber uzayda daha etkili ve acil pozisyon alınmasında ve milli güvenlik, milli eğitim, istihbarata karşı koyma, ekomonik – psikolojik – siyasi spekülatif siber uzay mecralı ataklara karşı kamu diplomasisi, eğitim ve toplumsal farkındalık şeklinde karşı tedbirlerin

sahada daha etkili olmasında siber savunma kuvvetlerinin teknik kabiliyetleri kadar önemli olduğu atmosferde bu önerinin şeklen ve usulen değerlendirmeye alınmasında fayda olduğu düşünülmektedir.

Bu önerinin temel gerekçesi, Türkiye'nin mevcut siber güvenlik eğitim ve politika çerçevesindeki önemli boşluklardan kaynaklanmaktadır. Önemli yatırımlara rağmen, Türkiye siber saldırılara karşı oldukça savunmasızdır ve bu durum büyük ölçüde bireysel düzeyde yetersiz siber güvenlik eğitimi ve parçalı politika uygulamalarından kaynaklanmaktadır. Özel daire başkanlıklarının kurulması, çabaları, kaynakları ve uzmanlığı merkezileştirerek bu sorunları gidermeyi hedeflemektedir.

Önerilen Eğitim, Farkındalık ve Güvenlik Odaklı Siber Uzay Faaliyetleri Daire Başkanlıkları, siber güvenlik girişimlerinin kapsamlı denetimi ve yönetimi sağlamak üzere yapılandırılmalıdır. Ana fonksiyonlar şunları içermelidir:

Politika Geliştirme ve Uygulama: Ulusal ve uluslararası standartlarla uyumlu siber güvenlik politikalarının oluşturulması ve uygulanması.

Eğitim ve Farkındalık Programları: Kamu sektörü çalışanlarının siber güvenlik farkındalık ve becerilerini artırmak için hedeflenmiş eğitim programlarının geliştirilmesi ve sunulması.

Olay Müdahale ve Yönetimi: Siber olaylara hızlı müdahale için tespit, sınırlama ve iyileştirme protokollerinin oluşturulması.

Araştırma ve Geliştirme: Yeni ortaya çıkan siber tehditleri önceden tespit etmek ve riskleri azaltmak için yenilikçi çözümler geliştirmek üzere araştırma yapılması.

İşbirliği ve Koordinasyon: Kamu kurumları arasında, özel sektör ve uluslararası kuruluşlarla bilgi ve en iyi uygulamaların paylaşımını kolaylaştırmak.

Beklenen Faydalar

Eğitim, Farkındalık ve Güvenlik Odaklı Siber Uzay Faaliyetleri Daire Başkanlıklarının kurulması birkaç önemli fayda sağlayacaktır:

Güçlendirilmiş Güvenlik Duruşu: Merkezileşmiş yönetim, siber güvenlik konusunda daha bütüncül ve etkili bir yaklaşım sağlayarak zafiyetleri azaltacak ve müdahale sürelerini iyileştirecektir.

Geliştirilmiş Eğitim ve Farkındalık: Özel daire başkanlıkları, bireysel düzeydeki siber güvenlik eğitimindeki mevcut boşlukları ele alarak tutarlı ve kapsamlı eğitim sağlayabilecektir.

Proaktif Tehdit Yönetimi: Araştırma ve geliştirme odaklı çalışmalar, olaylar gerçekleştikten sonra müdahale etmek yerine, yeni tehditleri proaktif olarak tespit etmeye ve azaltmaya odaklanacaktır.

Artan İşbirliği: Kamu kurumları ve diğer paydaşlar arasındaki yapılandırılmış koordinasyon, bilgi ve kaynakların paylaşımını kolaylaştırarak daha dirençli bir siber güvenlik altyapısı oluşturacaktır.

Uygulama Önerisi

Bu öneriyi hayata geçirmek için aşağıdaki adımlar atılmalıdır:

Mevzuat Çerçevesi: Kamu kurumları bünyesinde Eğitim, Farkındalık ve Güvenlik Odaklı Siber Uzay Faaliyetleri Daire Başkanlıklarını kuracak mevzuatın geliştirilmesi ve yürürlüğe konulması.

Kaynak Tahsisi: Bu dairelerin kurulması ve işletilmesi için gerekli kaynakların, finansman ve personel dâhil, tahsis edilmesi.

Paydaş Katılımı: Geniş destek ve iş birliği sağlamak amacıyla, hükümet birimleri, özel sektör ortakları ve uluslararası kuruluşlar gibi kilit paydaşlarla etkileşimde bulunulması.

İzleme ve Değerlendirme: Dairelerin etkinliğini değerlendirmek ve gerekli düzenlemeleri yapmak için sürekli izleme ve değerlendirme mekanizmalarının oluşturulması.

Kamu kurumları bünyesinde Eğitim, Farkındalık ve Güvenlik Odaklı Siber Uzay Faaliyetleri Daire Başkanlıklarının kurulması, Türkiye'nin siber güvenlik çerçevesini güçlendirme yolunda kritik bir adım teşkil etmektedir. Mevcut boşlukları ele alarak koordinasyon ve uzmanlığı artırmak suretiyle, bu daireler dijital çağda ulusal güvenliğin sağlanmasında hayati bir rol oynayacaktır.

Bu yapılanma, siber güvenlik önlemlerinin etkinliğini artırmada önemli bir rol oynayacaktır. Tabii ki bu yapılanmanın; Cumhurbaşkanlığı bünyesinde siber uzaya dair birçok alana dair sorumlulukları barındırmakta olan hâlihazırdaki Dijital Dönüşüm Ofisi Başkanlığı'ndan ayrı planlanacak doğrudan Cumhurbaşkanı'na bağlı yeni bir başkanlık tahsisi ile daha da güçlendirilmesi mümkün olacaktır. Bu alan tartışmalı ve her gün yeni gelişmelerle koşullarının değişebileceği bir mahiyettedir. Özellikle yapay zeka teknolojilerindeki evrime şahitlik ettiğimiz bu günlerden geleceğe yönetsel karar destek sistemlerinin nerelere evrilebileceğini elbette kestiremeyiz. Ancak söz konusu alan siber uzay olunca artık sadece insanlardan teşekkül edilen kurullar, başkanlıklar, komisyonlar yeni dünya düzeninde eksik kalacaktır. Yapay zekâdan destek alınmadan artık politika geliştirmenin ve bu politikaların hayata geçirilmesinin, takibinin değerlendirilmesinin mümkün olamayacağı bir eşikte bulunmaktayız. Bu yeni duruma uyum sağlayan hatta öncü olabilen devletler, kuruluşlar, şirketler ve bireyler her alanda olduğu gibi siber uzay alanında da hem güvenlik hem de kazanımlar manasında mukayese edilemeyecek üstünlükler kazanacaklardır. Elbette bu yeni aktör yani insanın yanında artık bir sanal bir koltuğun, sanal bir sümen takımının bulunacağının yani yapay zekâ ehli bir siber uzay teknolojisinin ön görülemez faydaları olacağı kadar öngörülemez yıkıcılığının da olabileceği her disiplinde olması gerektiği gibi uluslararası ilişkiler disiplininde de hele ki politika geliştirme süreçlerinde artık göz ardı edilemez.

KAYNAKÇA

ACM. (2017). *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity.* Joint Task Force on Cybersecurity Education. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Agaba, A. (2020). *Tailored Security Awareness Training: A Strategic Approach.* LinkedIn. https://www.linkedin.com/pulse/tailored-security-awareness-training-strategic-approach-agaba-allan

Akyeşilmen, N. (2016a). Cybersecurity and human rights: Need for a paradigm shift? *Cyberpolitik Journal, 1*(1), 32-48. http://www.cyberpolitikjournal.org

Akyeşilmen, N. (2016b). Türkiye in the global cybersecurity arena: Strategies in theory and practice. *Cyberpolitik Journal, 1*(1), 49-65. http://www.cyberpolitikjournal.org

Akyeşilmen, N. (2019). Rethinking cybersecurity: A quick transformation. International Journal of Cyber Studies, 2(3), 176-182. http://www.cyberstudiesjournal.org

Akyeşilmen, N. (2022). Türkiye in the global cybersecurity arena. *Insight Turkey*. https://www.jstor.org/stable/48733380

Al-Janabi, S., & AlShourbaji, I. (2015). A study of cybersecurity awareness in educational environment in the Middle East. *Journal of Information Security*, *6*(3), 206-214.

Aldirasa. (2024). *Cybersecurity major in detail: Its advantages and areas of work.* https://www.aldirasa.com/en/faqs/cyber-security-major-faq

Ankara Üniversitesi. (2023). *Siber güvenlik eğitimi ve programları.* https://siber.ankara.edu.tr

ASELSAN. (n.d.-a). *Siber teknolojiler.* https://www.aselsan.com/tr/savunma/kategori/10/siber-teknolojiler?content=kripto-ve-bilgi-guvenligi-sistemleri

ASELSAN. (n.d.-b). *Kripto ve bilgi güvenliği sistemleri*. https://www.aselsan.com/tr/savunma/kategori/10/siber-teknolojiler?content=kripto-ve-bilgi-guvenligi-sistemleri

Asia-Pacific Economic Cooperation (APEC). (2021). APEC Cybersecurity Strategy. https://ccdcoe.org/uploads/2018/10/APEC-020823-CyberSecurityStrategy.pdf

AustCyber. (2021). *Schools cyber security challenges*. https://www.austcyber.com/resources/dashboards/cyber-security-challenges

Austin, G. (2020). *Cyber security education: Principles and policies*. New York, NY: Routledge.

Australian Centre for Cyber Security (ACCS). (2019). *Enhancing national cyber defense capabilities*. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Baykar Milli MTAL. (2024a). *Aday öğrencilerimize açık mektup*. MEB. https://baykar.meb.k12.tr/icerikler/aday-ogrencilerimize-acik-mektup_15315210.html

Baykar Milli MTAL. (2024b). *Okulumuz hakkında*. MEB. https://baykar.meb.k12.tr/34/36/774333/okulumuz_hakkinda.html

Bayraktar, G. (2015). *Siber Savaş ve Ulusal Güvenlik Stratejisi*. İstanbul: Yeniyüzyıl Yayınları.

Beghe Sönmez, S., & Karakaşlar, M. (2023). *Cybersecurity: Turkey 2023*. Law Business Research. https://paksoy.av.tr/wp-content/uploads/2024/06/LBR-Law-Business-Research-Getting-the-Deal-Through-Cybersecurity-Turkey-2023.pdf

Białoskórski, R. (2012). Cyberthreats in The Security Environment of The 21st Century: Attempt of The Conceptual Analysis. *Journal of Security and Sustainability. 1*(4), 249-260. https://doi.org/10.9770/jssi.2012.1.4

Bıçakçı, S. (2013). *21. Yüzyılda siber güvenlik*. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Bilkent University. (2023). *Bilgisayar Mühendisliği Bölümü*. https://cs.bilkent.edu.tr

Boğaziçi Üniversitesi (2023). https://bogazici.edu.tr/

Boğaziçi Üniversitesi Siber Güvenlik Merkezi. (t.y.). *Siber Güvenlik Merkezi*. https://siber.bogazici.edu.tr/tr#:~:text=Hedeflerimiz,bir%20proje%20olarak%20hayata%20ge%C3%A7mi%C5%9Ftir

Borowski, C., Diethelm, I., & Wilken, H. (2016). What children ask about computers, the Internet, robots, mobiles, games etc. In *Proceedings of the 11th Workshop in Primary and Secondary Computing Education* (pp. 72-75). https://doi.org/10.1145/2978249.2978259

Brzostek, A. (2022). Germany's cybersecurity policy. *Teka Komisji Prawniczej PAN Oddział w Lublinie, 15*(2), 61–72. https://doi.org/10.32084/tkp.4793

BTK Akademi. (n.d.-a). *BTK Akademi hakkında*. BTK Akademi. https://www.btkakademi.gov.tr/

BTK Akademi. (n.d.-b). *Eğitim programları*. BTK Akademi. https://www.btkakademi.gov.tr/portal/coursecontentlist?programId=1

BTK Akademi. (2021). *Ulusal Siber Kalkan 2021 Tatbikatı*. BTK Akademi. https://www.btkakademi.gov.tr/portal/announcements

BTK Akademi. (2024). *8. Hacktrick Siber Güvenlik Konferansı ve 7. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi*. BTK Akademi. https://www.btkakademi.gov.tr/portal/announcements

Cartwright, E., Hernandez Castro, J., & Cartwright, A. (2019). To pay or not: Game theoretic models of ransomware. *Journal of Cybersecurity*, 5(1).

Cavelty, M. D. (2015). Cybersecurity. In A. Collins (Ed.), *Contemporary security studies* (pp. 400-416). Oxford University Press. ISBN: 9780198862192

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011, July). Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)* (Vol. 1). The Steering Committee of The World Congress in Computer Science Computer.

Cisco. (2023). *Cisco cybersecurity training programs.* https://www.cisco.com/site/us/en/learn/training-certifications/training/index.html

Clark, A. (2024). *Cybersecurity in the UK.* Commons Library Research Briefing. https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf

Clarke, R., & Knake, R. K. (2010). Siber Savaş Ulusal Güvenliğe Yönelik Yeni Tehdit (M. Erduran, Çev.). İstanbul: İKÜ Yayın Evi.

Clemente, D., Livingstone, D., Cornish, P. & Yorke, C. (2010). *On cyber warfare: A Chatham House report.* Chatham House.

CoHE. (2023). *Council of Higher Education and Information Technologies and Communications Authority sign protocol.* https://www.yok.gov.tr/en/Sayfalar/news/2024/council-of-higher-education-and-information-technologies-and-communications-authority-sign-protocol.aspx

Cyber Security Educational Curriculums in Turkey. (2016, May). *Conference: International Conference on Research in Education and Science; At: Bodrum; Volume: 3.*

Cybersecurity & Infrastructure Security Agency (CISA). (2021). *Cyber essentials: Implementing strong cybersecurity practices.* https://www.cisa.gov/resources-tools/resources/cyber-essentials

Çakır, H., & Taşer, M. (2023). Türkiye'de yapılan siber güvenlik faaliyetlerinin ve eğitim çalışmalarının değerlendirilmesi. *Gazi University Journal of Science Part C: Design and Technology, 11*(1), 1-11.

Çakmak, H., & Altunok, T. (2009). *Suç, terör ve savaş üçgeninde siber dünya.* Ankara: Barış Platin Kitabevi.

Çakmak, H., & Demir, C. K. (2009). Siber dünyadaki tehdit ve kavramlar. In H. Çakmak & T. Altınok (Eds.), *Suç, terör ve savaş üçgeninde siber dünya* (1. baskı, pp. 23-55). Ankara: Barış Platin Kitabevi.

Çifci, H. (2013). *Her yönüyle siber savaş.* Ankara: TÜBİTAK.

Çitlioğlu, E. (2008). *Gri tehdit terörizm.* Ankara: Başak Matbaacılık ve Tanıtım Ltd. Şti.

Daily Sabah. (2021). Turkey's cyber fortress fights digital threats around-the-clock. https://www.dailysabah.com/turkey/turkeys-cyber-fortress-fights-digital-threats-around-the-clock/news

Daily Sabah. (2023). 4 Turkish universities to launch vocational cybersecurity schools. https://www.dailysabah.com/turkiye/education/4-turkish-universities-to-launch-vocational-cybersecurity-schools

Dakota, C. (2021). China's national cybersecurity center. Center for Security and Emerging Technology, July 2021. https://doi.org/10.51593/2020CA016

Darıcılı, A. B. (2019). Türkiye'nin siber güvenlik politikalarının analizi; Türkiye'nin siber güvenlik modeli için öneriler. *Tesam Akademi Dergisi, 6*(2), 11-33. http://dx.doi.org/10.30626/tesamakademi.613517

Department of Defense. (2010). *Quadrennial defense review report.* Washington, DC: Department of Defense. https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf

Department of Homeland Security (DHS). (2020). *Actions needed to improve CyberCorps Scholarship for Service Program CyberCorps®: Scholarship for Service.* https://www.gao.gov/assets/d22105187.pdf

Düveroğlu, E. (2020). *A comparative analysis of critical infrastructure cyber security policies: Best practices from the US, EU, and Turkey.* Bilkent University. https://repository.bilkent.edu.tr/server/api/core/bitstreams/8a80e845-daea-4ea9-86c8-14428a3bb16c/content

EC-Council. (2024). *Cybersecurity certification courses in Turkey.* https://www.eccouncil.org/cybersecurity-courses-and-training-in-turkey/

Eitan, O. (2018). Turkey: Challenges to the struggle against cyber threats. *Cyber Intelligence and Security*, *2*(1), 39-53. https://www.inss.org.il/wp-content/uploads/2018/05/Turkey%E2%80%94Challenges-to-the-Struggle-against-Cyber-Threats.pdf

Emniyet Genel Müdürlüğü. (2022)., *Uluslararası Eğitim Kataloğu*. https://www.egm.gov.tr/siber/egitimler

Ermağan, İ. (2022). *Uluslararası ilişkiler ve teknoloji ilişkisi: Endüstri 4.0, siber uzay ve uzay dünyası*. 1. Baskı. Nobel: Ankara.

Ermağan, İ. (2024). *Türkiye'nin kurtuluş reçetesi: Teknoloji, Endüstri 4.0* [Video]. Herkekolog. YouTube. https://www.youtube.com/watch?v=tPnLDszFpGQ

Eskici, B. (2019). *Mini bilgisayarların ortaokullarda bilişim teknolojileri ve yazılım derslerinde kullanılması: Hibrit bilişim sınıfı örneği.* (Yüksek lisans tezi, İstanbul Üniversitesi, İstanbul). https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=-0-4acHpe02lyVBxiuqRVg&no=atLTsnLbjU3n8EVDnyLG7A

European Commission. (2020). *Digital education action plan (2021-2027).* https://education.ec.europa.eu/focus-topics/digital-education/action-plan

European Commission. (2013). *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace.* https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Union Agency for Cybersecurity (ENISA). (2020). *Cybersecurity education in the EU.* https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/

European Union Agency for Cybersecurity (ENISA). (2021). *European cyber security month.* https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month

European Union Agency for Cybersecurity (ENISA). (2022). *Cybersecurity education initiatives in the EU member states.* https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states

European Union Agency for Cybersecurity (ENISA). (2022). *European cybersecurity skills development in EU.* https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

European Union External Action Service. (2023). The European Union and NATO intensify cooperation on addressing cyber threats. https://www.eeas.europa.eu/eeas/european-union-and-nato-intensify-cooperation-addressing-cyber-threats_en

Federal Ministry of the Interior Building and Community. (2021). *Cyber security strategy for Germany 2021.* https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=81C7B4ED015E7BA904D87CC0981D0E94.live871?__blob=publicationFile&v=5

Federal Office for Information Security (BSI). (2023). *IT security situation in Germany 2023.* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf

Forum of Incident Response and Security Teams (FIRST). (2021). *About FIRST.* https://www.first.org/about/

Gazi Üniversitesi. (2023). *Siber Güvenlik Araştırma ve Geliştirme Topluluğu.* https://topluluklar.gazi.edu.tr/view/page/189076

Gazi Üniversitesi. (2023). *Gazi Üniversitesi web sitesi.* https://gazi.edu.tr/

Gazi Üniversitesi Fen Bilimleri Enstitüsü. (t.y.). *Misyon - Vizyon.* https://fenbilimleri.gazi.edu.tr/view/page/247728

Gazi Üniversitesi Fen Bilimleri Enstitüsü. (t.y.). *Genel Bilgiler.* https://fenbilimleri.gazi.edu.tr/view/page/247729

Gazi Üniversitesi. (t.y.a). *Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı.* https://obs.gazi.edu.tr/oibs/bologna/index.aspx?lang=tr&curOp=showPac&curUnit=83&curSunit=833939239#

Gazi Üniversitesi. (t.y.b). *Bilgi Güvenliği Mühendisliği Doktora Programı.* https://obs.gazi.edu.tr/oibs/bologna/index.aspx?lang=tr&curOp=showPac&curUnit=83&curSunit=833939218#

Global Forum on Cyber Expertise (GFCE). (2021). *Cyber capacity building.* https://thegfce.org/project/establishment-of-a-global-forum-on-cyber-expertise-pacific-hub/

Gordon, M. S. (2018). *Economic and national security effects of cyber attacks against small business communities* (M.S. thesis, Utica College, Utica, NY, USA) [ProQuest Dissertations Publishing, Art. no. 10935780].

Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022–2030. (2022). https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

Göçoğlu, V. (2018). *Türkiye'nin siber güvenlik politikalarının kamu politikası analizi çerçevesinde değerlendirilmesi*. (Yayınlanmamış doktora tezi, Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara). https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=KesFoJdA5T9qfGrY4vRgGg&no=UK4XyiRPwiYj1ekpmJos_w

Gündüz, M. Z., & Daş, R. (2018). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 24*(2), 327-335.

Hadnagy, C. (2010). *Social engineering: The art of human hacking.* Indianapolis: Wiley.

Halisdemir, E. (2021). *National cybersecurity organisation: Turkey.* NATO Cooperative Cyber Defence Centre of Excellence. https://www.ccdcoe.org/uploads/2021/08/TUR_country_report_final_clean_ver_2408.pdf

Hartikainen, H., Livari, N., & Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction, 22,* 1-16. https://doi.org/10.1016/j.ijcci.2019.100146

HAVELSAN. (n.d.-a). *Siber güvenlik.* https://www.havelsan.com.tr/sektorler/siber-guvenlik/siber-guvenlik

HAVELSAN. (n.d.-b). *Kurumsal hakkında.* https://www.havelsan.com.tr/kurumsal/hakkimizda/misyon-ve-vizyon-degerler-ve-amaclar

ISPI. (2022). *In cybersecurity, Turkey leads the way.* https://www.ispionline.it/en/publication/cybersecurity-turkey-leads-way-35348

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Information Security Education and Awareness (ISEA). (2020). *Promoting cybersecurity awareness in India.* https://isea.gov.in/

Insight Turkey. (2022). *Türkiye in the global cybersecurity arena: Strategies in theory and practice.* https://www.insightturkey.com/articles/turkiye-in-the-global-cybersecurity-arena-strategies-in-theory-and-practice

Insight Turkey. (2023). *Türkiye in the global cybersecurity arena: Strategies in theory and practice.* https://www.insightturkey.com/articles/turkiye-in-the-global-cybersecurity-arena-strategies-in-theory-and-practice

International Association of Privacy Professionals (IAPP). (2021). *Data privacy and cybersecurity training programs.* https://iapp.org/train/

International Information System Security Certification Consortium (ISC)². (2020). *Certified information systems security professional (CISSP).* https://www.isc2.org/certifications/cissp

International Institute for Strategic Studies. (2023). *Cyber capabilities and national power: Volume 2: Türkiye.* IISS. https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/

International Telecommunication Union (ITU). (2021). *Global cybersecurity agenda.* https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

International Telecommunication Union. (2014). *Cyberwellness profile: Turkey*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Turkey.pdf

Internet Society (ISOC). (2020). *Online Trust Alliance*. https://www.internetsociety.org/ota/

Invest in Turkey. (2023). *2023 vision to be realized with new national cybersecurity strategy*. https://www.invest.gov.tr/en/news/news-from-turkey/pages/2023-vision-to-be-realized-with-new-national-cybersecurity-strategy.aspx

İstanbul İl Milli Eğitim Müdürlüğü. (2018). *Siber güvenlik ve sosyal medyanın doğru kullanımı çalıştayları kitabı*. https://istanbul.meb.gov.tr/yegitek/pdf/siber/calistay_1_2_kitabi.pdf

İstanbul Üniversitesi (2023). *İstanbul Üniversitesi web sitesi*. https://www.istanbul.edu.tr/tr

İstanbul Üniversitesi-Cerrahpaşa. (2023a). *Siber güvenlik yüksek lisans programı*. https://ebs.iuc.edu.tr/home/program/?id=4l3DFNXxzuc%3d&yil=2023

İstanbul Üniversitesi-Cerrahpaşa. (2023b). *Siber güvenlik yüksek lisans programı eğitim amaçları*. https://ebs.iuc.edu.tr/home/amachedef/?id=4l3DFNXxzuc%3d

İstanbul Üniversitesi-Cerrahpaşa. (2023c). *Ders programı*. https://ebs.iuc.edu.tr/home/dersprogram/?id=4l3DFNXxzuc%3d&yil=2023

İstanbul Üniversitesi-Cerrahpaşa. (2023d). *Bölümümüz - tarihçe*. https://bilgisayarmuhendislik.iuc.edu.tr/tr/content/bolumumuz/tarihce

İstanbul Üniversitesi-Cerrahpaşa. (2023e). *2023-2024 ders planı*. https://cdn.iuc.edu.tr/FileHandler2.ashx?f=2023-2024-ders-plani-yeni.pdf

İstanbul Teknik Üniversitesi. (2024). *Siber Güvenlik Mühendisliği Lisans Programı*. İTÜ. https://bbf.itu.edu.tr/egitim/lisans/siber-g%C3%BCvenlik-m%C3%BChendisli%C4%9Fi

İstanbul Teknik Üniversitesi. (2024a). *İTÜ Siber Güvenlik Meslek Yüksekokulu Tercih 2024* [Video]. YouTube. https://www.youtube.com/watch?v=vT9hi3t8jYU

İstanbul Teknik Üniversitesi. (2024b). *İTÜ Siber Güvenlik Mühendisliği Tercih 2024* [Video]. YouTube. https://www.youtube.com/watch?v=q9LYQnLSAc8

İTÜ Siber Güvenlik Meslek Yüksekokulu. (2023). *İTÜ Siber Güvenlik Meslek Yüksekokulu*. https://sgmyo.itu.edu.tr/

Karabulut, Y. E., Boylu, G., Küçüksille, E. U., & Yalçınkaya, M. A. (2015). Characteristics of cyber incident response teams in the world and recommendations for Turkey. *Balkan Journal of Electrical & Computer Engineering, 3*(4), 175-178. https://dergipark.org.tr/tr/download/article-file/458525

Karataş, A. (2020). The comparative analysis of national cyber security policies: United States, United Kingdom, and Turkey examples. *Academic Social Resources Journal, 5*(19), 737-751.

Kaspersky. (2021). *Cybersecurity awareness training: Building a cyber-resilient workforce.* https://www.kaspersky.com/enterprise-security/security-awareness

Koç Üniversitesi. (2023). https://www.ku.edu.tr/

Koç Üniversitesi. (2024). *Cyber security - Courses.* Koç Üniversitesi Fen Bilimleri Enstitüsü. https://gsse.ku.edu.tr/en/programs/cyber-security/courses/

Kovács, L. (2018). Cyber security policy and strategy in the European Union and NATO. *Land Forces Academy Review, XXIII*(1), 15-24. https://www.researchgate.net/publication/325147671_Cyber_Security_Policy_and_Strategy_in_the_European_Union_and_Nato

Kurnaz, S., & Önen, S. M. (2019). Avrupa Birliğine uyum sürecinde Türkiye'nin siber güvenlik stratejileri. *International Journal of Politics and Security (IJPS), 1*(2), 82-103.

Lavie-Dinur, A., Aharoni, M., & Karniel, Y. (2021). Safe online ethical code for and by the 'net generation': Themes emerging from school students' wisdom of the crowd. *Journal of Information Communication and Ethics in Society, 19*(1), 129-145. https://doi.org/10.1108/JICES-02-2020-0021

Lexology GTDT. (2022). *Cybersecurity in Turkey*. https://www.lexology.com/panoramic/tool/workareas/report/cybersecurity/chapter/turkiye

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND Corporation.

Liszkowska, D. (2024). Turkey's cybersecurity policy framework. *Cybersecurity and Law*. https://bibliotekanauki.pl/articles/31341977.pdf

Lu, M., & Reeves, J. (2014). Types of cyber attacks. *Trustworthy Cyber Infrastructure for the Power Grid, 18,* 2017. http://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf

McAfee. (2020). *Cybersecurity awareness month: If you connect it, protect it.* https://www.mcafee.com/blogs/internet-security/cybersecurity-awareness-month-if-you-connect-it-protect-it/

Miller, R. L., & Meshkat, L. (2022). A systems approach for cybersecurity risk assessment. *2022 Annual Reliability and Maintainability Symposium (RAMS).*

Milli Savunma Üniversitesi. (2023). *Ders Kapsam Kitabı 2023-2024.* https://atasaren.msu.edu.tr/contents/akademik/dersicerikleri/Ders_Kapsam_Kitabi_2023_2024.pdf

Milli Savunma Üniversitesi. (n.d.-a). *Bilgisayar mühendisliği bölümü.* https://kho.msu.edu.tr/akademik/dekanlik/bilgisayar_bolumu/siberguvenlik_abd.html

Milli Savunma Üniversitesi. (n.d.-b). *KHO genel bilgi.* https://kho.msu.edu.tr/hakkinda/Kho_genel_bilgi.html

Milli Savunma Üniversitesi. (n.d.-c). *Siber Güvenlik Yüksek Lisans Programı*. https://kho.msu.edu.tr/akademik/enstitu/belgeler/ders_konu_kapsamlari/Bilgisayar%20M%C3%BChendisli%C4%9Fi%20ABD/Siber%20G%C3%BCvenlik%20Y%C3%BCksek%20Lisans%20Program%C4%B1.pdf

Ministry of Electronics and Information Technology (MeitY). (2013). *National Cyber Security Policy*. https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

National Cyber Security Centre (NCSC). (2021). *Cyber Aware*. https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Cyber%20Aware&sort=date%2Bdesc

National Institute of Electronics & Information Technology (NIELIT). (2021). *Cybersecurity education and training programs*. https://www.nielit.gov.in/haridwar/content/online-courses

National Institute of Standards and Technology (NIST). (2017). *National Initiative for Cybersecurity Education (NICE)*. https://www.nist.gov/system/files/documents/2019/11/08/nist.sp_.800-181.pdf

NCIA. (n.d.). *NCI Academy*. NATO Communications and Information Agency. https://www.ncia.nato.int/what-we-do/nci-academy.html

Nguyen, T. A., & Pham, H. (2020, October). A design theory-based gamification approach for information security training. In *2020 RIVF international conference on computing and communication technologies (RIVF)* (pp. 1-4). IEEE.

ODTÜ. (2023). https://kim.metu.edu.tr/tr/ogrenci-topluluklari#siber

Organization for Economic Co-operation and Development (OECD). (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. https://www.oecd.org/en/publications/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc.html

Orta Doğu Teknik Üniversitesi. (t.y.). *Siber Güvenlik Yüksek Lisans Programı*. https://ii.metu.edu.tr/tr/siberguvenlik-ms

Ozztech. (2022). *Etkili bir siber güvenlik politikası nasıl oluşturulur?* https://www.ozztech.net/siber-guvenlik/etkili-bir-siber-guvenlik-politikasi-nasil-olusturulur/

Özker, U. (2022). *Critical infrastructure and cyber security in Türkiye.* Konrad-Adenauer-Stiftung e.V. and Centre for Economics and Foreign Policy Studies (EDAM). https://www.kas.de/documents/283907/283956/KAS+x+EDAM_%C3%96zker_Critical+Infrastructure+and+Cyber+Security+in+T%C3%BCrkiye.pdf

Pernik, P. (2014). *Improving cyber security: NATO and the EU.* International Centre for Defence Studies. https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, 1-25. https://doi.org/10.1016/j.ijcci.2021.100343

Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics, 177*, 351–374. https://doi.org/10.1007/s10551-020-04717-9

Rahman, N. A. A., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10*(5), 378-382.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7-8), 241-253.

Rodríguez-de-Dios, I., & Igartua, J. J. (2016). Skills of digital literacy to address the risks of interactive communication. *Journal of Information Technology Research, 9*(1), 54-64. https://doi.org/10.1007/978-3-030-51974-2_19

Sabancı Üniversitesi. (2023). https://www.sabanciuniv.edu/tr

Saeed, S. (2023). Education online presence and cybersecurity implications: A study of information security practices of computing students in Saudi Arabia. *Sustainability, 15*(12), 9426. https://doi.org/10.3390/su15129426

SANS Institute. (2024). *Cybersecurity certifications.* SANS Institute. https://www.sans.edu/cyber-security-programs/undergraduate-certificate/

Savunma Sanayii Akademisi. (2024a). *Türk savunma sanayii'nde nitelikli insan kaynağı geliştirme platformu.* https://www.ssa.gov.tr/

Savunma Sanayii Akademisi. (2024b). *Siber güvenlik eğitim programı.* https://www.ssa.gov.tr/egitim-programlari/5-siber-guvenlik-egitim-programi

Sayedi, S. O. (2020). *Ulusal siber güvenlik stratejisi oluşturma süreç analizi ve Türkiye ile Afganistan'ın ulusal siber güvenlik stratejisinin değerlendirilmesi* (Yüksek lisans tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü). https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=wf-FPgY-5qjHEzEoOgvMs4bf5F3pWwop_c9fdNh1He76PddyLxcb5HxQ_DM2ypw_

Schlienger, T., & Teufel, S. (2003). Information security culture - From analysis to change. *South African Computer Journal, 31,* 46-52.

Schreider, T. (2020). *Cybersecurity law standards and regulations.* Rothstein Publishing.

Shafi, Q. (2012). Cyber physical systems security: A brief survey. In *Computational Science and Its Applications (ICCSA) IEEE 12th International Conference on* (pp. 146-150).

Siber Güvenlik Eğitim Portalı. (n.d.-a). *Eğitim Katalogları.* Siber Güvenlik Eğitim Portalı. https://www.siberguvenlikportal.org/kataloglar

Singer, P. W., & Friedman, A. (2015). *Siber güvenlik ve siber savaş* (A. Atav, Çev.). Ankara: Buzdağı Yayın Evi.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Spoclearn. (2024). *Cybersecurity courses & certification Turkey.* https://www.spoclearn.com/tr/courses/cybersecurity/

STM ThinkTech. (2020). *Siber güvenlikte insan faktörü.* https://thinktech.stm.com.tr/tr/siber-guvenlikte-insan-faktoru

Švábenský, V., Vykopal, J., & Čelada, P. (2020). What are cybersecurity education papers about: A systematic literature review of SIGCSE and ITiCSE conferences. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (pp. 2-8). https://doi.org/10.1145/3328778.3366816

Taylor-Jackson, J., McAlaney, J., Foster, J. L., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating psychology into cyber security education: A pedagogical approach. In M. Bernhard et al. (Eds.), *Financial cryptography and data security: FC 2020* (Lecture Notes in Computer Science, Vol. 12063). Springer, Cham. https://doi.org/10.1007/978-3-030-54455-3_15

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2023). Siber Güvenlik. https://cbddo.gov.tr/siber-guvenlik/

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2020). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. https://cbddo.gov.tr/siber-guvenlik-stratejisi/

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi.* https://hgm.uab.gov.tr/strateji-eylem-planlari

Teknopark İstanbul MTAL. (2024). *Okulumuzun öyküsü.* Millî Eğitim Bakanlığı. https://teknoparkistanbul.meb.k12.tr/icerikler/okulumuzun-oykusu_9760323.html

Teknopark İstanbul MTAL. (2019). *Bir meslek alanı olarak siber güvenlik çalıştayı.* Teknopark İstanbul. https://teknoparkistanbul.meb.k12.tr/meb_iys_dosyalar/34/16/767393/dosyalar/2023_02/17125544_2019-Bir-Meslek-Alani-Olarak-Siber-Guvenlik-Calistayi.pdf

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi. (2021). *2021-2022 Brifing dosyası.* https://teknoparkistanbul.meb.k12.tr/meb_iys_dosyalar/34/16/767393/dosyalar/2022_07/06201056_2021-2022-Brifing-Dosyasi.pdf?CHK=33b68cca9c7e6ed6eb9ce47ef13b1ee3

The National Cyber Security Centre (NCSC). (2020). CyberFirst: Empowering the Next Generation of Cybersecurity Professionals. https://www.ncsc.gov.uk/cyberfirst/overview

The White House. (2003). The national strategy to secure cyberspace. Washington, DC: The White House.

Trade.gov. (2024). Turkey - Information and Communication Technology. https://www.trade.gov/country-commercial-guides/turkey-information-and-communication-technology

TÜBİTAK BİLGEM. (2023). UEKAE Trainings. TÜBİTAK. https://bilgem.tubitak.gov.tr/en/trainings/sge-education/

TÜBİTAK. (2023). Cyber Security Training Programmes. TÜBİTAK. https://bilgem.tubitak.gov.tr/en/trainings/

TÜBİTAK. (n.d.-a). *Siber Güvenlik Eğitim ve Araştırma Merkezi Projesi.* TÜBİTAK. https://www.tubitak.gov.tr/tr/kurumsal/uluslararasi/icerik-siber-guvenlik-egitim-ve-arastirma-merkezi

TÜBİTAK. (n.d.-b). *Siber Güvenlik Eğitim Portalı.* TÜBİTAK. https://www.siberguvenlikportal.org

TÜBİTAK. (2022). *Siber Güvenlik Projeleri Destekleri.* TÜBİTAK. https://www.tubitak.gov.tr/tr/duyuru/siber-guvenlik-projeleri-destekleri

TÜBİTAK BİLGEM. (2024). *Ana Sayfa.* TÜBİTAK BİLGEM. https://bilgem.tubitak.gov.tr/

Türkiye Bilişim Derneği. (2023). https://www.tbd.org.tr/

Türkiye Siber Güvenlik Kümelenmesi. (n.d.-a). *Hakkımızda.* https://siberkume.org.tr/hakkimizda

Türkiye Siber Güvenlik Kümelenmesi. (n.d.-b). *Kariyer.* https://siberkume.org.tr/kariyer

Türkiye Siber Güvenlik Kümelenmesi. (n.d.-c). *Eğitim.* https://siberkume.org.tr/egitimler

Türkiye Siber Güvenlik Kümelenmesi. (n.d.-d). *Katalog.* https://siberkume.org.tr/katalog?page=1

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2013). *Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı*. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar. (2012). *T.C. Resmî Gazete*, 28447, 20 Ekim 2012. https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf

United Nations Office on Drugs and Crime (UNODC). (2021). *Global Programme on Cybercrime*. https://www.unodc.org/westandcentralafrica/en/Cyber-Crime.html

United States Cyber Command (USCYBERCOM). (2021). *Integrating Cybersecurity Education in Military Training*. https://www.cybercom.mil/

USMA (United States Military Academy). (2016). *Academic Program: Class of 2020 Curriculum and Course Descriptions (Red Book)*. www.westpoint.edu/academics/dean/strategic-documents

Ülgen, S., Kim, G., Bıçakcı, S., Çelikpala, M., Han, A. K., Kasapoğlu, C., & Ergun, F. D. (2015). *A primer on cyber security in Turkey and the case of nuclear power*. Centre for Economics and Foreign Policy Studies (EDAM). https://dergipark.org.tr/tr/download/article-file/458525

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Bilgi Teknolojileri ve İletişim Kurumu.

Vasileiou, I., & Furnell, S. (Eds.). (2019). *Cybersecurity education for awareness and compliance*. IGI Global.

von Solms, S., & von Solms, R. (2014). Towards cyber safety education in primary schools in Africa. In *Proceedings of the 8th International Symposium on Human Aspects of Information Security Assurance* (pp. 185-197). https://www.cscan.org/openaccess/?id=247

Wang, S., Wang, W., Guan, S., & Guan, N. (2019). Research on cyberspace security education for teenagers based on data analysis. In *Proceedings of the International Conference on Information Technology and Electrical Engineering* (pp. 1-3). https://doi.org/10.1145/3386415.3386971

Yazıcı, A. (2011). *Siber Güvenlik ve SAHAB.* Elektrik Mühendisleri Odası. http://www.emo.org.tr/ekler/fad64faae21db53_ek.pdf

Yıldız Teknik Üniversitesi. (2023a). https://yildiz.edu.tr/

Yıldız Teknik Üniversitesi. (2023b). *Fen Bilimleri Enstitüsü Yüksek Lisans Programları.* https://fbe.yildiz.edu.tr/page/GRADUATE-ADMISSIONS/MSc--PROGRAMS/144

Yükseköğretim Kurulu [YÖK]. (2024). *Türk üniversitelerinin dünya sıralamasındaki dikkat çekici yükselişi sürüyor.* https://www.yok.gov.tr/Sayfalar/Haberler/2024/turk-universitelerinin-dunya-siralamasindaki-dikkat-cekici-yukselisi-suruyor.aspx#:~:text=%C4%B0lk%201000'de%20yer%20alan901%2D950%20band%C4%B1nda%20yer%20ald%C4%B1

Zhang-Kennedy, L., & Chiasson, S. (2020). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys, 54*(1), 1-39. https://doi.org/10.1145/3427920

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı	: Burak ESKİCİ
Uyruğu	: T.C.
Doğum Tarihi ve Yeri	:
Elektronik Posta	:

EĞİTİM

Derece	Kurum	Mezuniyet Yılı
Lisans	Yıldız Teknik Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü	2008
	Anadolu Üniversitesi, İktisat Fakültesi, Uluslararası İlişkiler Bölümü	2013
Yüksek Lisans	İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Enformatik Anabilim Dalı	2019
	İMÜ, Lisansütü Eğitim Enstitüsü, Uluslararası İlişkiler Anabilim Dalı	2024

İŞ TECRÜBESİ

Tarih	Kurum	Görev
2023- Devam	Yıldız Teknik Üniversitesi	Öğretim Görevlisi
2008- Devam	Milli Eğitim Bakanlığı	Uzman Öğretmen

YABANCI DİLLER

İNGİLİZCE (YÖKDİL 85)

YAYINLAR

Ayvaz Reis, Z., Göcükoğlu, B., & Eskici, B. (2014). İşitme ve Konuşma Engellilerin Yaşamlarını Kolaylaştırma. *XVI. Akademik Bilişim Konferansı Bildirileri*, 215-222. https://ab.org.tr/kitap/ab14.pdf

Eskici, B. (2019). *Mini bilgisayarların ortaokullarda bilişim teknolojileri ve yazılım derslerinde kullanılması: Hibrit bilişim sınıfı örneği.* (Yüksek lisans tezi, İstanbul Üniversitesi, İstanbul). https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=-0-4acHpe02lyVBxiuqRVg&no=atLTsnLbjU3n8EVDnyLG7A

Eskici, B. (2020), "*Ortaokullarda Bilişim Teknolojileri Eğitimi Ortamı Eksikliğine Bir Çözüm Önerisi Olarak Hibrit Bilişim Sınıfı Modeli*", 8th International Conference on Future Learning and Informatics: Data Revolution. 20-22 October, 2020 (e-Conference)

Eskici, B. (2024). *Siber güvenlik politikalarında eğitim ve Türkiye'nin siber güvenlik eğitimi politikası*. (Yüksek lisans tezi, İstanbul Medeniyet Üniversitesi, İstanbul).