İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

İstanbul Commerce University Journal of Science

http://dergipark.org.tr/ticaretfbd

Araştırma Makalesi / Research Article

SİBER GÜVENLİK ALANINDA NİTELİKLİ İŞ GÜCÜ YETİŞTİRMEK İÇİN BAYRAĞI YAKALA YARIŞMASI YAKLAŞIMI*

CAPTURE THE FLAG COMPETITION APPROACH TO EDUCATE QUALIFIED WORKFORCE IN CYBER SECURITY

Cafer ULUÇ[1] **Can EYÜPOĞLU**[2]

https://doi.org/10.55071/ticaretfbd.1529412

Sorumlu Yazar ***(Corresponding Author)***	***Geliş Tarihi*** ***(Received)***	***Revizyon Tarihi*** ***(Revised)***	***Kabul Tarihi*** ***(Accepted)***
cafer@tutanota.com	*06.08.2024*	*13.09.2024*	*18.09.2024*

Öz

Kara, deniz, hava ve uzay, savaşın dört boyutu olarak kabul edilir. Görece yakın sayılacak bir dönemde harbin beşinci boyutu olarak kabul edilen siber uzay, kendisinden önce anılan dört boyutu da etkileme kapasitesine sahiptir. Günümüz çatışmalarının ve dahi savaşların etkili bir aktörü olan bu sahadaki etkin duruşun sağlanması ise kuşkusuz nitelikli insan gücünün varlığıyla olasıdır. Siber güvenlik gibi disiplinler arasılığı bünyesinde barındıran bir alanda profesyonel düzeyde uzman yetiştirmenin zorluğu bilinmektedir. Siber güvenliğin eğitim yaklaşımında ise alanın dinamiklerine uygun bir metodoloji ortaya konması gerekliliği ortaya çıkmaktadır. Bu araştırmanın sonucunda varılan noktada ulusal güvenliğin yeni bir unsuru olan siber uzaya devletlerin kamu ve ordu düzeyinde verdiği önceliklerle siber güvenlik eğitiminin aynı zamanda bir devlet politikası olduğu görülmüştür. Bu noktada siber güvenlikte nitelikli iş gücünün yetiştirilmesine yönelik yaklaşımların dünyada ve Türkiye'deki yerini araştırmanın yanı sıra bir eğitim önermesine de bu çalışmada yer verilmektedir.

Anahtar Kelimeler: Siber güvenlik eğitimi, siber güvenlikte iş gücü, bayrağı yakala yarışması, ulusal güvenlik.

Abstract

The four dimensions of war are land, sea, air and space. In a relatively recent period, the fifth dimension of warfare, cyber space, has been accepted as a fifth dimension of warfare. This has the capacity to affect the four dimensions mentioned before it. It is possible to ensure an effective stance in this field, which is an effective actor in today's conflicts and even wars, with the presence of qualified manpower. It is widely acknowledged that it is challenging to train experts at a professional level in an interdisciplinary field such as cyber security. In the context of cyber security education, it is essential to develop a methodology that aligns with the dynamic nature of the field. This research has revealed that cyber security education is also a state policy, with the priorities set by the states regarding cyber space, which is a novel element of national security at both the public and military levels. In addition to investigating the place of approaches to the training of a qualified labour force in cyber security in the world and in Türkiye, this study also includes an educational proposal.

Keywords: Cyber security education, workforce in cyber security, capture the flag, national security.

* *Bu yayın Cafer ULUÇ isimli öğrencinin Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Siber Güvenlik Programındaki Yüksek Lisans projesinden üretilmiştir.*

[1] Teknopark İstanbul, İstanbul, Türkiye.
Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği ABD, İstanbul, Türkiye.
cafer@tutanota.com, Orcid.org/0000-0003-4756-5757.

[2] Milli Savunma Üniversitesi, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye.
ceyupoglu@hho.msu.edu.tr, Orcid.org/0000-0002-6133-8617.

1. GİRİŞ

Siber güvenlik alanı, ülkelerin en üst düzeyde varlıklarını etkin ve güçlü olarak göstermek durumunda oldukları dijital bir sahadır. Bu yeni alan kara, deniz, hava ve uzay kadar ulusal güvenliğin sağlanmasıyla doğrudan ilgilidir.

Türkiye'de siber güvenlik çerçevesinde ilk strateji belgesi 2013'te T.C. Ulaştırma ve Altyapı Bakanlığınca yayınlanmıştır. "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013) sonucunda siber güvenlikle ilgili kamu kurumlarının kurulmasına karar verilmiştir. Yanı sıra 2015'te, Birleşik Krallık'ta yayınlanan "Ulusal Güvenlik Stratejisi ve Stratejik Savunma ve Güvenlik İncelemesi" (Government of the United Kingdom, 2015) adlı belgede siber tehditler, "Birinci Kademe Risk" olarak derecelendirilmiştir (Haggman, 2019). 2016 yılında ABD'de yayınlanan "Siber Güvenlik Ulusal Eylem Planı"nda (Ford ve ark., 2017) siber güvenlik, ABD'nin karşı karşıya olduğu en önemli zorluklardan biri olarak ifade edilmektedir.

Ulusal ve uluslararası literatür çalışması sonucunda güvenlik paradigmalarının bütününü etkileyen bir konumda olan siber uzayda görevlendirilecek nitelikli iş gücüne yönelik ciddi çalışmaların olduğu görülmekle birlikte alanın görece yeni olması ise siber güvenlik alanında yetiştirilecek nitelikli iş gücünün eğitim ve öğretimine yönelik yaklaşımların henüz gidecek çok yolun olduğu görülmektedir.

Bu çalışma, dünyada ve Türkiye'de siber güvenlik alanında nitelikli iş gücü yetiştirme yaklaşımlarını incelenmektedir. Yapılan incelemelerin yanı sıra bir eğitim modeli önerisinde bulunulmaktadır. Söz konusu yaklaşım ise terimsel olarak Capture the Flag (CTF) adıyla bilinen Bayrağı Yakala Yarışması'dır (BYY). Farklı kıtalardan farklı ülkelerin akademik ölçekteki çalışmaları incelenmiş olup dünyanın farklı coğrafyalarındaki siber güvenlikte uzman yetiştirme perspektifine bir bakış ortaya konması amaçlanmaktadır.

2. GENEL BİLGİLER

Bu bölümde BYY hakkında genel bilgiler ortaya konacaktır. BYY'nin tarihsel geçmişi, kazanımları ve Türkiye'de düzenlenen "Liseler Arası Bayrağı Yakala Yarışmaları"na değinilecektir.

2.1. Bayrağı Yakala Yarışması

Capture the Flag'in bir kısaltması olan CTF, Türkçede "Bayrağı Yakala", "Bayrak Kapmaca" ve "Bayrağı Yakala Yarışması" gibi karşılıklarla anılır. Türkçe literatürde ve sahada yaygın olarak CTF olarak bilinir. Bununla birlikte Türkçe kısaltmasının işleklik kazanması önemlidir. Bu bağlamda çalışma boyunca BYY kısaltmasının kullanımı tercih edilecektir.

Genel bir açıklamayla BYY, siber güvenlik alanındaki yetkin kişilerin, kurgulanmış senaryolardaki soruları çözerek becerilerini gösterebildiği bir tür teknik yarışmadır. Mücadeleye dayalı olarak süren BYY'ler aynı zamanda kişiye farklı bakış açıları

kazandıran yönü de içinde barındırır. Katılımcı, soruları çözdüğünü kanıtlamak adına sorunun içerisinde yer alan metin tabanlı ifadeye ulaşarak ilgili bölüme bunu ekler ve böylece bayrağı yakalamış/kapmış olur.

Her bayrak, sorunun zorluk düzeyine göre değişken bir puanlamaya sahiptir. Yarışmacı tek başına olabileceği gibi takım halinde de katılarak yarışabilirler. Belli bir sürenin sonunda yarışma biter ve en çok puanı toplayan kişi ya da takımlara organizasyonu düzenleyenlerce belirlenen ödüller verilir.

Bayrağı yakala yarışmalarının kendi içinde bir bayram biçimi bulunmaktadır. Genel bir bayrak biçimi ise şöyledir: *flag{Düz_Metin}.* "flag" sözcüğü, BYY'yi düzenleyenlere göre değişebilmektedir.

Bayrağı yakala terimi, fiziksel olarak iki takım arasında oynana açık hava oyununda kullanılır. Amaç, karşı rakibin bayrağını (gizlenmiş de olabilir) ele geçirirken aynı zamanda kendi bayrağını da karşı takımdan korumayı içerir.

1993 yılında ilk defa DEFCON'da düzenlenen yarışmada bu terim siber uzaya taşınmış oldu (Švábenský ve ark., 2020). DEFCON başladığında bir grup siber güvenlik uzmanının ilgisi dahilindeydi. Çok geçmeden özel sektörün ve kolluk güçlerinin de ilgisini çekmeye başladı (Katzcy Consulting, 2016).

Aradan geçen otuz yıldan sonra hacking temalı konferanslar ve BYY'ler yalnızca uzmanları değil yeni başlayan kişiler için de bir giriş kapısı olma niteliği taşıyabilmektedir. Özellikle oyunlaştırma yaklaşımları dünya çapındaki öğretmenlerin eğitim müfredatında elini güçlendiren bir yöntem olarak işlevsellik göstermektedir (Švábenský ve ark., 2020).

Chung ve Cohen (Chung & Cohen, 2014) çalışmalarında BYY'yi satranca benzetmektedirler. Yazarlar, kuralların basit olduğunu ancak ustalaşmanın uzun yıllara dayanan bir deneyim gerektirdiğine dikkat çekmektedir.

2.1.1. Kazanımları

Siber güvenlikte nitelikli personel açığını kapatmada siber güvenlik yarışmaları tek başına yeterli olmayabilir. Bu kabulle birlikte yarışmaya katılanlar özenle hazırlanmış simülasyonlarda gerçek dünya sorunlarına benzer olarak uygulamalı deneyimleri edinebilmektedirler (Katzcy Consulting, 2016). BYY'ler, okul temelinde ele alındığında sınıf içinde ya da ders kitaplarındaki teorik konuların pratiğe dökülmesine zemin hazırlar. Normal şartlarda riskli olabilecek saldırı ve savunma durumlarını güvenli bir sanallaştırma ortamında sınamalarına olanak tanınır. Böylece katılımcılar, tutuklanma ve yargılanma gibi herhangi bir yasal endişe duymaksızın saldırıları gerçekleştirebilirler (Davis ve ark., 2014). Pedagojik açıdan değeri son zamanlarda daha fazla öne çıkan BYY'ler, katılımcılarına uygulamalı güvenlik becerilerini deneyimleme şansı sağlar (Wi ve ark., 2018). Buradan hareketle bir öğretim aracı olarak BYY, öğrencinin performansına yönelik anlık geri bildirimler sunarak artı ve eksi yönlerin ortaya konmasında öğrenciye yol gösterebilir. Öğrencinin derste gördüğü konuları gerçek hayatla bir bağ kurabilmesi önemli bir ayrıntıdır (Leune & Petrilli, 2017). BYY'ler, uygulama alanı sunabilen bir formata sahip olduğundan öğrenciye

teoride gördüğü konuları pratikte uygulayabileceği bir ortam sunabilmektedirler. Gardner'ın "Çoklu Zeka Kuramı"nda ortaya koyduğu üzere her kişinin zeka türü çeşitlilik gösterebilmektedir. BYY'ler bu çoklu sunum yönüyle öğrenime yüksek katkı sağlayabilmektedirler.

BYY'ler, katılımcısına bilişim sistemlerine yapılan saldırı vektörlerini tanıma noktasında katkı sağlayabilmektedirler. Bununla birlikte BYY'ler katılımcısına, ilgili sistemlerin nasıl savunulabileceğine yönelik etkili bir bakış kazandırabilmektedirler.

BYY'ler, geleceğin siber güvenlik profesyonellerini ve liderlerini hazırlamasında önemli bir katkıları vardır (Albert & Wallingford, 2010). BYY'de başarı gösteren öğrencilere burs, staj ve iş fırsatları sunulmaktadır (Cherinka & Prezzama, 2015; Conti ve ark., 2011; Davis ve ark., 2014; Raman ve ark., 2014). Geleceğin iş gücüne katkı sağlamak için BYY'leri bir araç olarak değerlendirirken aynı zamanda mevcuttaki siber güvenlik uzmanlarının güncel kalması ve yeteneklerini yükseltme olanağı da tanımaktadır (Katzcy Consulting, 2016). BYY'ler kurum, kuruluş ve şirketler için yetenekli kişilerin işe alımı için iş verenlere uygun ortamlar sunmaktadır (Matias ve ark., 2018). BYY'lere katılım ve elde edilen başarılar, iş verenin işe alım sürecinde kişinin teknik becerileri hakkında temel bir görüş sağlar (Chung, Lowering the Barriers to Capture The Flag Administration and Participation, 2017). Bu yönüyle de bayrağı yakala yarışmalarına katılmak, kişinin saygınlığına da katkı sağlar (Conti ve ark., 2011).

BYY'ler iş verenlerin potansiyel olarak istihdam edecekleri iş gücüyle buluşmaları için bir tür alan da sağlayabilmektedir. Buna bir örnek olarak 2009 yılında ABD'de düzenlenen Ulusal Üniversite Siber Savunma Yarışması'nda Boeing firmasının BYY'de başarılı olanlara iş teklif etmesi verilebilir (Katzcy Consulting, 2016). Türkiye'de de benzer durumların yaşandığı bilinmektedir (Ünal, "Siber Yıldız" Olmak için 26 Bin Kişi Yarışacak, 2017).

Capture the Flag altyapısı sunan CTFd ekibinden Kevin Chung'ın da (Chung, Lowering the Barriers to Capture The Flag Administration and Participation, 2017) vurguladığı üzere BYY'ler, rekabetçi yönleri ve ekip halinde yarışma olanağı sunduklarından bilgi güvenliği sektörüne giriş olarak kabul edilir. Bayrağı yakala yarışmalarının ve buna yönelik platformların artmasıyla siber güvenlik alanına giriş engeli azalacaktır.

BYY'ler, yetkin kişilerin aralarında yarıştığı ve bir tür gövde gösterisi yapıldığı eğlenceli ciddi oyunlardır. Katılımcılara farklı bakış açıları kazandıran bu tür yarışmaların yeni başlayanlar için de siber güvenliği bir giriş kapısı olacağı düşünülerek öne sürülen bu çalışma, siber güvenlik öğretiminde BYY'nin büyük bir potansiyele sahip olunduğu fikriyle ele alınmaktadır.

BYY'ler aynı zamanda ekip içi yönetim ve iş birliği gibi yeteneklerin de gelişimine katkı sağlayabilmektedir. Yanı sıra BYY'ler, *bir hacker nasıl düşünür*, bunu anlamak üzerine zihinsel bir beceri gelişimine zemin hazırlar, dahası, katkı sağlayarak bir bakış açısı kazandırır. Analiz kabiliyetine katkı sağlayan bu süreçte noktaları birleştirici bir perspektifle potansiyel olarak saldırganın düşünce yapısıyla konuya yaklaşım gösterebilir (Chase & Uppuluri, 2022; Eagle & Clark, 2004; Katsantonis ve ark., 2023; Katzcy Consulting, 2016; Li & Kulkarni, 2016; Rowe ve ark., 2011; Son ve ark., 2012;

Yasin ve ark, 2018). "Hacker bakış açısını edinmek" öylesine bir söylem değildir. Nitekim kötü niyetli bir saldırganın konuya olan yaklaşımını tanımak, gelebilecek olası saldırı vektörlerini kestirebilmenin etkili bir yoludur. Sivil güvenlik araştırmacılarının yanı sıra askeri akademideki araştırmacıların (Conti ve ark., 2011) da dikkat çektiği nokta budur.

Çin'de yerleşik Tsinghua Üniversitesinden (清华大学) Affan ve ark. (Yasin ve ark., 2018) 2018'de ele aldıkları çalışmada, oyuncuların bir saldırgan gibi düşünmelerini sağlayacak oyunlaştırılmış bir eğitim önermektedirler. Burada *hacker* ifadesini hangi amaçla kullanıldığına açıklık getirmekte yarar görünmektedir. Yaygın kanının aksine *hacker*, sistemleri bozan ve yıkıcı faaliyetleri gerçekleştiren kişi değil bilişim sistemlerini derinlemesine bilen, farklı bakış açılarıyla ortaya ürün/hizmet koyabilen üst düzey kabiliyete sahip bilgisayar uzmanıdır.

BYY'ye katılmanın öğrenci üzerindeki yararlarını sıralarken son olarak benzer ilgiye ve yönlere sahip kişilerin bir araya gelmesine olanak tanımasına değinmek gerekmektedir. Bir tür sosyal etkinlik olarak da görülebilecek olan BYY'ler, bu yönüyle katılımcısına bir tanışma ağı da sağlamaktadırlar (Eagle & Clark, 2004).

2.1.2. BYY platformları

Siber güvenliğe yeni başlayanların öğrendiklerini uygulayabileceği alanlar siber güvenliğin doğası gereği istenmeyen yasa dışı sonuçlara neden olabilmektedir. Konuyla ilgili halihazırda var olan laboratuvar ortamları ise özellikle siber güvenlik temelleri olmayan ya da yeni başlayan öğrencilerin gözünde büyüyebilmekte, heveslerinin kırılmasına neden olabilmektedir.

Var olan BYY'ler değerli bir çözüm olmalarının yanı sıra yeni başlayan bir öğrenci açısından yaklaşıldığında öğretim materyali olarak görülmekten uzaktırlar. Ayrıca yaygın olarak bilinen bu platformlarda ücretsiz olarak sunulanlar olsa da ağırlıklı olarak ücretlidir ve ek masraflar içerir. Bu dönem projesinde ortaya koyulan amaç doğrultusunda öğretim temelli başlıca bir BYY platformu geliştirilmesi önceliktir.

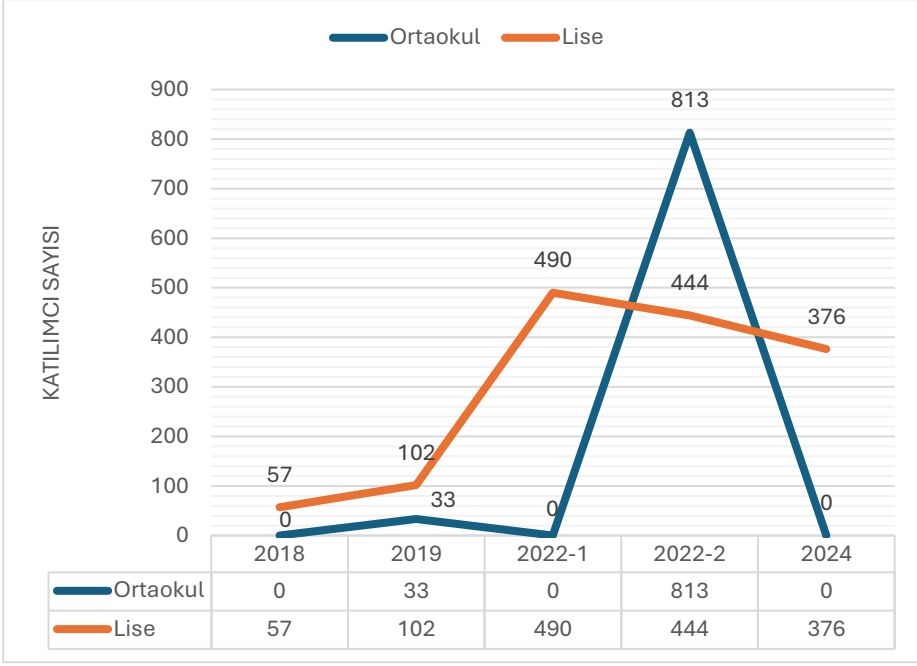
2.1.3. Liseler arası bayrağı yakala yarışması

20 Ocak 2017'de Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesindeki Ulusal Siber Olaylara Müdahale Merkezinin (USOM) "Siber Yıldız" adıyla düzenlediği BYY'ye yaklaşık 26.000 kişi başvuru yapmıştır. Bu başvurular incelendiğinde %84'ünün 18 yaş altında, %16'sının ise 13-14 yaş altında olduğu sonucuna varılmaktadır (Ünal, 2017). Bu verilerden hareketle bu projenin de odak kitlesi olarak belirlediği ilköğretim ve ortaöğretim öğrencilerinin ilgisinin ne denli olduğu açıkça görülebilmektedir.

Türkiye'de ortaöğretim düzeyinde siber güvenlik çalışmaları 2015'e değin gitmektedir. 2015-2016 eğitim ve öğretim yılında "LAB3: Liseler Arası Bilişim Kampı" adıyla başlatılan proje 2017'de İstanbul İl Milli Eğitim Müdürlüğünce siber güvenlik müfredatı ve siber güvenlik lisesi çalışmalarına evrilmiştir (Küçükçekmece İlçe Milli Eğitim Müdürlüğü, 2016) (Uluç, 2017). 15 Mayıs 2020 yılında ise bütünüyle siber

güvenlik eğitimi üzerine faaliyet göstermesi amacıyla Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi (2023) kurulmuştur.

Şekil 1'de "Liseler Arası Bayrağı Yakala Yarışmaları"na başvuran öğrencilerin sayıları yer almaktadır. 2018 ve 2019'daki yarışmalar İstanbul İl Milli Eğitim Müdürlüğü bünyesinde düzenlenmiştir. 2020'de Teknopark İstanbul MTAL kurulup eğitim ve öğretime başladıktan sonra söz konusu yarışma TİMTAL'in ana sorumluluğunda düzenlenmeye başlanmıştır.



Şekil 1. Yıllara göre Liseler Arası Bayrağı Yakala Yarışmalarına Başvuran Öğrenci Sayısı

Ortaokul öğrencilerinin 0 (sıfır) olarak görüldüğü 2018 ve 2022-1 yıllarında yarışma yalnızca liselere yönelik düzenlenmiştir. Küresel salgın Covid-19 nedeniyle 2020 ve 2021 yıllarında yarışma düzenlenememiştir. İlk üç yıldaki yarışmalar, İstanbul'daki okulların katılımıyla sınırlıdır. 2022-2'deki yarışma ise Türkiye genelindeki ortaokul ve lise öğrencilerinin katılımıyla çevrim içi olarak gerçekleştirilmiştir.

Savunma Sanayii Başkanlığı (SSB) ve Dijital Dönüşüm Ofisi Başkanlığı (DDO) koordinasyonunda Türkiye Siber Güvenlik Kümelenmesi tarafından "Siber Güvenlik Haftası" düzenlenmektedir. Hafta kapsamında, Teknopark İstanbul MTAL'nin hazırladığı ve 28-29 Kasım 2022'de çevrim içi düzenlenen BYY'lerde bireysel olarak 813 ortaokul, 444 lise olmak üzere 1.257 öğrenci bayrağı yakalamak için akranlarıyla yarışmıştır. 2024 yılında ise Cumhuriyetimizin ikinci 100 yılına özel olarak tüm Türkiye'den liselerin katılımına açık olarak düzenlenmiştir. "Cumhuriyetimizin İkinci 100 Yılında Bayrak Sende Türkiye" deyişiyle 25 Mayıs 2024'te ulusal ölçekte

gerçekleşen "5. Liseler Arası Ulusal Bayrağı Yakala Yarışması"na 46 farklı ilden 376 lise öğrencisi başvuru yapmıştır.

2.2. Ulusal Güvenlik Bağlamında Siber Uzay

Yeni teknolojilerin ülkelerin stratejik hedeflerinde yer almasıyla birlikte ordunun da saldırı ve savunma sistemleriyle entegresi yerleşmeye başladı ve böylece askeri anlamda savaşın sahası da genişlemiş oldu. Örneğin hava sahası, I. ve II. Dünya Savaşları'nda kara ve denizin yanı sıra yeni savaş alanı olarak varlık gösterdi. Soğuk Savaş'ın ardından ise uzay, Batı ve Doğu blokları arasında yeni nesil bir savaş alanı olarak görüldü. Takip eden süreçte elektronik bileşenlerin gelişimiyle birlikte bilgisayar ve İnternet'in git gide askeri ve sivilde yer edinmesiyle dijital varlıklar da ulusal güvenliğin bir parçası haline geldi. Bu gelişmeler doğrultusunda siber uzay; günümüzde kara, deniz, hava, uzaya ek olarak beşinci savaş alanı olarak değerlendirilmekte, her fırsatta güçlü bir vurguyla kendine yer bulabilmektedir (Dill, 2018).

Siber güvenliği yalnızca teknik bir disiplin olarak görmek bu noktadaki yaklaşımlarda eksikliklere neden olmaktadır. Konvansiyonel bir savaşta sahadaki askeri gücün varlığının yanı sıra cephe gerisindeki halkın duruşu da belirleyici bir unsurdur. Yanı sıra psikoloji, sosyoloji, ekonomi, bürokrasi ve diplomasi gibi faktörler de en az ordunun kapasitesi kadar etkili olabilmektedir. Dolayısıyla güvenlik, bütüncül bir bakışla konuya yaklaşımı gerekli kılmaktadır.

Güvenlik paradigmalarının dönüşümü, güvenliğin yalnızca ordunun ve kolluk güçlerinin geleneksel anlamda sorumluluk alanının dışında bir yaklaşımı zorunlu kıldığı bir dönemde, siber güvenlik de proaktif bir yaklaşımla sivil unsurları da sürece dahil etmektedir. MİT'in 2024'te yayınladığı "2023 Yılı Faaliyet Raporu"nda (Milli İstihbarat Teşkilatı, 2024) dikkat çekildiği üzere bölgesel ve küresel ölçekteki tehditlerin hibrit ve asimetrik boyut kazanması ulusal güvenliğin sağlanmasını giderek daha karmaşık biçime getirmektedir. Bu durumda geleneksel güvenlik anlayışlarının yetersiz kaldığı ve çağa uygun yaklaşımların uygulanmasına vurgu yapılmaktadır. Teşkilat, ilgili raporda siber güvenliğe ayrıca değinerek kurumun siber kapasitesinin güçlendirilerek yeni nesil teknolojik atılımlarla Siber Vatan'da da etkin varlık gösterildiğine işaret etmektedir.

Siber uzayın yapısı dijital olduğundan konvansiyonel harp unsurlarını görmek olası değildir. Bundan dolayı devlet ve devlet dışı aktörlerin siber gücüyle ilgili bir çıkarımda bulunmak isabetli olamamaktadır. Askeri doktrinleriyle saygınlık kazanan Prusyalı General Clausewitz'in şu sözü konuyu destekler niteliktedir: *"Tüm insan faaliyetleri açısından savaş, en çok bir kart oyununa benzer."*.

Siber güvenlik, yapısının yanı sıra doğrudan devlet ve devlet dışı aktörlerin sistemlerine dahi etki edebilecek düzeyde bir konumda olduğundan söz konusu unsurların korunmasına yönelik aksiyonlar karmaşıklık içerir. Bu noktada öğretici faaliyetlerde eğitim amaçlı içeriklerin öğrenciye aktarılmasında zorluklar yaşanması şaşırtıcı bir sonuç değildir. Temel amaç siber güvenlik teknolojilerinin ve güvenlik paradigmalarının öğrencide durumsal farkındalığını oluşturmak ve bir bakış açısı kazandırmak olmaktadır.

2007'deki Rusya'nın Estonya'ya düzenlediği siber saldırılar sonucu NATO'nun başkent Tallinn'e kurduğu ve Türkiye'nin de daimi bir temsilcisinin yer aldığı NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) ise Estonya'yı siber güvenlik tatbikatlarının merkez üssü konumuna getirmiştir.

Siber güvenliğin sağlanması, siber uzayın yapısı gereği yalnızca güvenlik güçlerinin üstlenebileceği bir çerçeve dışındadır. Kolluk güçlerinin yanı sıra akademi, sektör ve her bireyin bu noktada koordinasyonu gerekir. Nitekim yıllar geçtikçe tehdit düzeyi artarken zarar verici unsurları gerçekleştirmek için gereken teknik becerilerde yetkinliğin ölçüsü azalmaktadır. Dolayısıyla tehdidin nereden geleceği (devlet ya da devlet dışı) bilinmeyen bir yapı söz konusudur.

Günümüzde, dünyanın her tarafında ve her an siber saldırılar yaşanmaktadır. Her yıl artan boyutta ilerleyen bu saldırılara karşı koymak ve verilerin güvenliğini sağlamak isteyen kurum ve kuruluşlar için zorluklar da artmaktadır. Bu zorluklara karşı güvenlik ve bilişim teknolojileri personellerinin eğitilmesi gerekmektedir (Noor Azam & Beuran, 2018). 2011 yılında ABD'de gerçekleştirilen bir konferansta, akademik kurumların siber tehditlere karşı yetenekli öğrencilerin yetiştirilmesi, ABD ve müttefiklerinin egemenliğinin korunmasına yardımcı olacak biçimde kritik bir konumda değerlendirilmektedir. ABD, ülkesine yapılacak siber saldırıları bir savaş eylemi olarak değerlendirirken Birleşik Krallık'ın, gelişmiş bir askeri siber güvenlik kapasitesi için 2011 yılında 1 milyar dolarlık bir yatırım yaptığı belirtilmektedir (Rowe ve ark., 2011). Maurice ve ark. (Hendrix ve ark., 2016) makalelerinde belirttikleri üzere 2016 yılı için Birleşik Krallık Kabine Ofisinin verisine göre siber suçların ülke ekonomisine maliyeti yılda yaklaşık olarak 27 milyar pounddur. Ayrıca yazarlar, Birleşik Krallık'ın siber güvenlik alanındaki işe alımında oyunlaştırmanın kullanıldığına değinmektedirler. Araştırıldığında, bu oyunun Birleşik Krallık devletince desteklendiği (McGoogan, 2015) görülmektedir.

Dünya genelinde milyonu aşan boyutta siber güvenlik uzmanı eksikliğinden söz edilir. Bu derinlik kamu kurumları için daha fazladır çünkü nitelikli uzmanlara özel sektörde çeşitli olanaklarla birlikte yüksek maaşlar verilebilmektedir. Devlet kurumlarında ise standart bir maaş söz konusudur. Birleşik Krallık'taki bir çalışmada (Haggman, 2019) da buna değinilmekte, ordunun ve istihbarat teşkilatlarının bile özel sektördeki cezbedici maaşların kamuda olmayışına dikkat çekilmekte, bunun da nitelikli profesyonellerin kurum içinde istihdam edilememesi nedeniyle bir sorun olduğu vurgulanmaktadır.

Bilişim teknolojilerinin yapısı, onu sürekli gelişen ve dönüşen bir biçimde tutmaktadır. Nitekim böylesi bir sahada etkin yer almanın yolu da bu dinamizme uygun bir insan kaynağının varlığıyla mümkündür. Bu noktada ABD, özellikle kritik altyapılarının sürekli korunmasını sağlayabilecek nitelikli iş gücüne sahip olmak adına ciddi bir yapılanmaya gittiği görülmektedir. Siber güvenlik alanındaki mesleklere yönelik norm ve standartları oluşturan bir kurumun varlığı ABD'de görülmektedir. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST: National Institute of Standards and Technology) bünyesinde kurulan Ulusal Siber Güvenlik Eğitimi Girişimi (NICE: National Initiative for Cybersecurity Education) bulunmaktadır (Cusak, 2023). NICE devlet, akademi ve özel sektöre arasında bir iş birliği sağlayarak siber güvenlik eğitimi ve iş gücünün gelişimine odaklanan bir ortaklıktır (Katzcy Consulting, 2016).

Düzenlenen NICE konferanslarının temaları ise iş gücünü geliştirmek için paydaşların bir arada ortak çalışmalar yürütmesine olanak tanımak, bilimsel çalışmalar ortaya koymaktır. Bu çalışmanın ele alındığı 2024 yılı içerisinde bakıldığında NICE konferansı, 3-5 Haziran 2024 tarihinde Teksas'ta yapılmıştır. İlgili web sayfasında her yıl olmak üzere 2028 yılına kadar haziran ayı içerisinde gerçekleştirileceğine yönelik takvimin olması, NICE'nin istikrarlı çalışmalarına dikkat çekilmesi açısından önemli bir ayrıntıdır. 2024'te düzenlenecek olan konferansın (National Initiative for Cybersecurity Education, 2024) teması ise "Ekosistemin Güçlendirilmesi" ana başlığında siber güvenlik alanındaki iş gücü açığının giderilmesinde paydaşların bir araya getirilmesidir. Cusak'ın ele aldığı makalede (Cusak, 2023) aktardığı üzere NICE konferanslarında siber güvenlik eğitiminin liseden de önce ortaokul düzeyinden başlanmasına yönelik öneriler söz konusudur. İlgili konferansta gerçekleştirilen panellerin birinde *GenCyber* ve *Cyber Patriot* gibi BYY çalışmalarının basitleştirilerek ortaokul seviyesine çekilmesi ve öğrencilerine eğitimine katkı sağlayacak biçimde kullanılması vurgulanmaktadır. Böylece, yeni başlayan ve deneyimsiz öğrenciler göz önüne alınarak başarılı sonuçlara giden yolda başarısız olmalarına izin verilebilecektir.

ABD'deki çalışmalar incelendiğinde üniversiteden önce lise düzeyinde siber güvenlik eğitimlerinin ders içi ve ders dışı etkinliklerle gündemde tutulduğu görülmektedir. Yanı sıra ilkokul ve ortaokul düzeyinde de siber güvenlik çalışmalarının kamu kurumlarınca sorumluluk alanına alındığı da söz konusudur. Örneğin, ABD Hava Kuvvetleri, Cyber Patriot programını genişleterek ilköğretim öğrencilerine yönelik farklı konu modülleri hazırlamaktadır (Li & Kulkarni, 2016).

Cyber Patriot, 2009'da sekiz takımla faaliyetine başlamıştır. 2013 yılına ait bir çalışmada, havacılık ve savunma şirketi olan ve ABD ordusuyla iş birliğiyle bilinen Northrop Grumman tarafından 4,5 milyon dolar bağış yapıldığı kaydedilmektedir (Tadjdeh, 2013). Northrop Grumman, savunma sanayii şirketlerinin sıralamasını derlemede saygın bir yayın olan Defense News Top 100'de 3. sıradadır. Söz konusu listede (Defense News, 2024) ülkemizden de dört firma (ASELSAN, TUSAŞ, ROKETSAN, ASFAT) bulunmaktadır. Cyber Patriot, 2024 yılında halen faaliyetlerini sürdürmektedir.

ABD'deki askeri kurumlar akademik çalışmaları da finansal olarak desteklemektedirler. Örneğin, 2022 yılında yazılan ve liseler için siber güvenliği konu edinen iki makalede açık olarak şöyle yazmaktadır: *"Bu araştırma kısmen NSA (National Security Agency: Ulusal Güvenlik Ajansı), NSF (National Science Foundation: Ulusal Bilim Vakfı) ve Cypherpath tarafından finanse edildi."* (Chase & Uppuluri, 2022). Bir diğer makalede (Werther ve ark., 2011) ise ABD Hava Kuvvetleri tarafından desteklendiği yer almaktadır.

ABD Hava Kuvvetleri görev tanımına "siber uzay savunması" ekleyerek "siber komuta" yapısını oluşturmuştur. AFA, lise öğrencilerinin bilim ve teknoloji alanlarıyla birlikte siber güvenlik alanında çalışmalarına yönelik bir dizi programları düzenlemeye başladığı bilinmektedir. AFA, Teksas Üniversitesindeki Altyapı Güvence ve Güvenlik Merkezi (CIAS: Center for Information Assurance and Security) ve Uluslararası Bilim Uygulamaları Birliği (SAIC: Science Applications International Corporation) kurumlarıyla iş birliği içerisinde doğrudan lise öğrencilerine yönelik "Cyber Patriot" eğitim programını geliştirdiler ve bu programın ilki 2009 yılında gerçekleştirildi (White

ve ark., 2010). Siber güvenlik konusu ABD tarafında ulusal güvenliğin ayrılmaz bir parçası olarak görülmekte ve her uygun fırsatta buna dikkat çekilmektedir. Cyber Patriot'ın adlandırmasının da buna uygun olarak seçildiği görülmektedir. Türkçeye "Siber Vatansever" olarak çevrilebilmektedir. White ve ark. (2010) ilerleyen yıllarda öğrencilerin hangi kariyer planını seçerlerse seçsinler sonuç olarak Cyber Patriot'ta aldıkları eğitim sonucunda edindikleri becerilerin onlara ve ABD'ye yardımcı olacağını anımsatmaktadırlar.

Te-Shun ve Jones (Chou & Jones, 2018), ABD'nin siber güvenlik eğitimini birincil önceliği olarak belirlediğini ifade etmektedirler. ABD'de yalnızca eğitimle ilgili kamu kurumları değil askeri kurumlar da BYY etkinlikleri düzenlemekte ve diğer yarışmalara sponsor olmaktadırlar (Cooper & Harris, 2022). ABD Donanma Hava Harp Merkezi Eğitim Sistemleri Bölümünden Cooper ve Harris'in ele aldığı çalışmada (Cooper & Harris, 2022) BYY'nin öğrenimdeki yararlarının kabul edilmesiyle birlikte Savunma Bakanlığına (Department of Defense) bağlı kuruluşlar siber güvenlikteki iş gücünün oluşmasına bu gibi siber güvenlik yarışmalarının geliştirilmesinde de etkin olarak yer aldıklarına dikkat çekmektedir.

Siber güvenlik alanında profesyonel eksikliği birçok çalışmada dile getirilmektedir. Bu sorunu gidermek için yetenekli kişilerin siber güvenlik alanında kariyer hedefine yönlendirmek adına ABD'de birtakım çalışmalar yürütülmektedir (Ster, 2019). Siber güvenlik profesyonellerinin eksikliği 2019'daki bir çalışmada (Ster, 2019) belirtilmiş olup alana yönelik ilginin artırılması adına çalışmalar farklı bölgelerde sürdürülmeye ve çeşitlenmeye devam etmektedir. Oluşan profesyonel boşluğunu doldurmak adına Kaliforniya Siber Güvenlik Enstitüsü, eyalet bazında önemli kuruluşlardan biri olarak anılmaktadır. Enstitü, Kaliforniya Politeknik Eyalet Üniversitesine bağlıdır. Yarışmanın paydaşları arasında ABD'nin istihbarat ve güvenlik güçleri olan Ulusal Güvenlik Ajansı (National Security Agency), Ulusal Muhafız Bürosu (National Guard Bureau) ve Uzay Kuvvetleri (Space Force) bulunmaktadır (California Cybersecurity Institute, 2024).

Cyber Patriot, ABD Hava ve Uzay Kuvvetleri Birliğince yürütülen savunma odaklı bir siber güvenlik yarışmasıdır. Yarışmanın amacı, ABD'nin siber güvenlik iş gücüne yönelik artan ihtiyacı karşılamaktır. AFA, Cyber Patriot ile ulusal çapta lise öğrencilerine yönelik BYY düzenlemek amacıyla faaliyetine başlamıştır (Albert & Wallingford, 2010). 2024 yılı itibariyle 16. kez düzenlenecek olan Cyber Patriot, "Ulusal Gençlik Siber Eğitim Programı" olarak kendisini tanıtmaktadır. Lise öğrencileri hedefiyle başlayan proje genişleyerek güncelde ortaokul öğrencilerini de kapsamaktadır (Cyber Patriot, 2024). Yanı sıra ilkokul düzeyinde öğretim içerikleri de oluşturmaktadırlar (Cyber Patriot, 2024). Cyber Patriot, İç Güvenlik Bakanlığı (Department of Homeland Security) ve Amerikan Askeri Üniversitesi (American Military University) gibi kamu kurumu ve özel şirketlerin sponsorluğuyla yapılmaktadır. Açıklandığı kadarıyla (Cyber Patriot, 2024) -yapılan bağışlar ve devlet kurumlarının fonlarının dışında- yalnızca 2024'teki organizasyon için sponsorların katkılarıyla 515 bin dolar bütçe ile fonlanmaktadır.

Siber güvenlik her ne kadar teknik bir beceri istese de amacının güvenliği sağlamak olduğu göz ardı edilmemelidir. Nitekim güvenlik, farklı disiplinlerin bir aradalığıyla sağlamlık kazanır. Bunların en başında iletişim ve yönetim gelir ki güvenliği

sağlanması amaçlanan son kullanıcıya yönelik çözüm sunulabilsin. Saldırı tarafında olan bir siber güvenlik uzmanı nasıl düşünürse savunma tarafında çalışan siber güvenlik uzmanının da bu düşünce yapısına kavuşması gerekir. Bu da teknik ve duygusal empatiyle mümkün olabilmektedir. Yanı sıra geliştirilen sistemler ve günümüzde yapay zekanın etkin biçimde yer almasıyla insan faktörü belli bir ölçüde dışarıda tutulabilmektedir. Siber güvenlik söz konusu olduğunda ifade edilen şu meşhur sözde olduğu gibi *güvenlikte en zayıf halka insandır.* Fakat sistemler her ne kadar gelişirse gelişsin, teknik istihbarat alanında olduğu gibi, insan temelli istihbarat belirleyici ve karar verici noktadadır. Siber güvenlik konusunda da benzer bir yaklaşım yanlış olmayacaktır. Anımsanmalıdır ki bir savaş oyunu, belirli bir stratejiyi ya da aracı test etmekten ötede sağladığı daha önemli bir yönü vardır: O stratejiyi/aracı uygulayacak olan insanı sınamak (Haggman, 2019).

Kanada Siber Güvenlik Merkezi tarafından hazırlanan raporda (Canadian Centre for Cyber Security, 2022) siber tehdit aktörleri ve motivasyonları şöyle açıklanmaktadır:

- Ulus devletlerin siber tehdit aktörleri genellikle jeopolitik motivasyona sahiptir.
- Siber suçlular genellikle finansal motivasyona sahiptir.
- Hacktivistler genellikle ideolojik motivasyona sahiptir.
- Terörist gruplar genellikle ideolojik şiddet motivasyonuna sahiptir.
- Heyecan arayan maceraperestler genellikle tatmin ile motive olurlar.
- İçeriden gelen tehdit aktörleri genellikle hoşnutsuzlukla motive olurlar.

Siber uzayın yapısı gereği savaştan ziyade bir mücadele ortamı olarak tanımlanmasını gerekli kılmaktadır. Literatürde sıklıkla geçtiği üzere *siber savaş* terimi, Milli İstihbarat Teşkilatının hazırladığı "MİT Sözlük"te (Milli İstihbarat Teşkilatı, 2024) şöyle ifade edilmektedir: "Zarar vermek, manipüle etmek, kendi çıkarları çerçevesinde kullanmak, kesinti yaratmak, tamamen hizmet veremez duruma getirmek üzere gerçekleştirilen saldırı faaliyetlerinin tümü.". Clarke'a göre (LeClair, Abraham, & Shih, 2013) ise siber savaş, bir devletin başka bir ülkenin bilgisayarlarına ya da ağlarına zarar vermek veya kesintiye neden olmak amacıyla sızma eylemleridir. 2007'de Rusya tarafından Estonya'ya ve ABD-İsrail tarafından İran'a düzenlenen siber ataklar bir ülkenin başka bir ülkenin kritik altyapılarına yönelik düzenlediği etki düzeyi yüksek saldırılar olarak örnek verilebilir. 2010 yılında dönemin ABD Başkanı Obama, ülkesinin dijital altyapılarını "stratejik ulusal varlık" olarak ilan etmiş olması (The Economist, 2010), alana yönelik verilen kritik hassasiyeti ortaya koyması açısından önemlidir.

ABD ordusundan Yarbay Karen J. Dill'in ele aldığı bir çalışmada (Dill, 2018) siber uzayın askeri yönüne dikkat çekilmektedir. ABD Başkanı tarafından Savunma Bakanlığına ve ilgili kamu kuruluşlarına siber güvenlik profesyonellerinin eğitimi ve işte tutulması konusunda uzun vadeli bir yol belirleme talimatı verildiğine vurgu yapılmaktadır. ABD'de yürütülen bir doktora tezinde (Wagner, 2023) siber güvenlik alanındaki uzman eksikliğinin ulusal güvenliği riske atacak durumda olduğu ifade edilmektedir. ABD, ulusal hedeflerini korumak adına siber uzaydaki yeteneklerini güçlendirmek adına sivil ve ordu kurumlarıyla siber güvenlikte nitelikli iş gücü için yetenek havuzunu güncel tutmaya çalışmaktadır (Dill, 2018). Siber güvenlik alanında nitelikli uzman açığı birçok çalışmada yinelenmektedir. Bu açığı kapatmaya yardımcı

olmak için ABD Hava Kuvvetleri Birliği, siber güvenlik alanında çalışan vasıflı bireylerin sayısını artırmak amacıyla 2008 yılında Cyber Patriot (Manson ve ark., 2012) yarışmasını tasarladı ki daha öncesinde söz konusu yarışma üzerine ayrıntılı bilgiye önceki sayfalarda değinilmişti.

Siber güvenlikte etkin bir konumda olmak, konuyla ilgili uluslararası niteliklerde gerek akademik gerek teknik çalışmalarla mümkün olmaktadır. Konu kapsamında bir örnek olarak 2004'te ABD tarafından kararlaştırılan ekim ayı kapsamında "Siber Güvenlik Farkındalık Ayı" (Cybersecurity and Infrastructure Security Agency, 2024) çeşitli etkinliklerle gündeme gelmektedir. Siber güvenlik çalışmalarında ABD ordusunun ve güvenlik birimlerinin öncülüğünde ilerlemektedir. Bu durum şaşırtıcı değildir nitekim hem bilgisayarın hem de İnternet'in çıkışı askeri amaçlar doğrultusunda ortaya konmuştur.

ABD Donanma Yüksek Okulunun bir girişimi olan *CyberCIEGE*, siber güvenlik eğitimi için hazırlanan bir video oyunudur. Yanı sıra Avrupa ülkelerinin bölgesel olarak iş birlikleri içerisinde siber güvenlik eğitiminde güç birliği sağlamaktadırlar. COLTRANE adındaki proje, Erasmus+ programı kapsamında beş ülkenin (Avusturya, Finlandiya, İtalya, Hollanda ve Birleşik Krallık) katkısıyla oluşturulan bir siber güvenlik farkındalığı eğitim topluluğudur (Langner ve ark., 2021).

Bir bütün olarak *siber güvenlik* terimi, içinde barındırdığı güvenlik yaklaşımlarından dolayı, askeri ve kolluk kuvvetlerinin alanında değerlendirilebilir. Nitekim siber uzayın temellerinin atıldığı İnternet, tam da böyle bir ortamda, ABD ordusuna bağlı Savunma İleri Düzey Araştırma Projeleri Ajansında (DARPA: Defense Advanced Research Projects Agency) ARPANET (Advanced Research Projects Agency Network: İleri Düzey Araştırma Projeleri Ajans Ağı) adıyla ortaya çıktı. Daha da geriye gidildiğinde ise bilgisayar sistemlerinin askeri bir gerekçeyle II. Dünya Savaşı sırasında ortaya çıktığı bilinmektedir. 1936 yılında Kondrad Zuse tarafından ilk programlanabilir bilgisayar olan Z3, Almanlarca şifreli yazılar üretmek için kullanılmaktaydı. Daha bilindik olan ENIAC (Electronic Numerical Integrator and Computer: Elektronik Sayısal Entegratör ve Hesaplayıcı) ise modern bilgisayarın ilk ürünü olarak kabul edilmektedir. ENIAC da ABD ordusunun isteği üzerine 1947 yılında füze ve top atışlarının hesaplanması için John Mauchly ve J. Presper Eckert öncülüğünde geliştirilmişti.

NATO'nun Estonya'nın başkenti Tallinn'de bulunan Siber Savunma Mükemmeliyet Merkezinin (Cooperative Cyber Defence Centre of Excellence) 2010'da düzenlemeye başladığı Kilitli Kalkan (Locked Shields) (The NATO Cooperative Cyber Defence Centre of Excellence, 2024) siber tatbikatına 2014'ten bu yana Türkiye'den TSK Siber Savunma Komutanlığının yanı sıra ilgili kamu ve özel sektör temsilcileri katılım sağlamaktadır (T.C. Milli Savunma Bakanlığı, 2023). Buradan hareketle varılabilecek sonuçlardan biri de Bayrağı Yakala Yarışması'nın eğitim ve öğretimdeki yaygınlığıyla birlikte etkisinin de oldukça geniş olduğudur.

Yukarıdaki örneklerle ortaya konulduğu üzere ulusal güvenlikle ilgili sanal ve fiziki unsur ayırt etmeksizin sıcak çatışmalar ya da askeri operasyonlar ordu ve kolluk güçlerinin birincil sorumluk alanında değerlendirilmektedir. Söz konusu siber uzay olduğunda ise güvenlik, çok katmanlı yapısı dolayısıyla toplumun bütünüyle doğrudan

ilgili olmaktadır. Yanı sıra dijital teknolojilerin doğası, alan üzerinde yüksek niteliklerle spesifik çalışmalar yürütebilen uzmanları gerekli kılmaktadır. Gelişmiş ülkelerde ordu ve emniyetin içinde yetişen mühendis sınıflarının yanı sıra akademisyen ve teknik bireylerin iş birliğiyle çalışmalar yapılmaktadır. Siber güvenlik, elbette yalnızca ordu ve emniyetin sorumluluk alanında tutulabilecek bir saha değildir. Nitekim akıllı telefonlar ve Nesnelerin İnternet'i (IoT: Internet of Things) teknoloji yaygınlaşmasıyla birlikte bilişim teknolojileri yalnızca askerinin/emniyetin hizmetinde değil her bir vatandaşın evindeki süpürgeye, mutfak gereçlerine, cebindeki telefona, odasındaki lambaya, bileğindeki saate, kapısındaki kilide ve dahi kişilerin organlarına değin girmiş durumdadır. Klasik savaşlar ya da sıcak çatışmalardan önce siber savaşlar yaşanmakta ve kimileyin de savaş ortamı konvansiyonel olarak ortaya çıkmadan uzun süre ülkeler arasındaki mücadele siber uzayda güç yarışına evrilebilmektedir. İşbu gerekçeler nitelikli insan gücünün ne denli önemli olduğunu ortaya koymaktadır. Nitelikli insan gücünün var olması da formal ve informal öğretim içerikleri ve öğretmenlerin varlığıyla mümkün olabilmektedir.

2.3. Türkiye'nin Siber Güvenlik Alanındaki Nitelikli İş Gücü Politikası

Dil, toplumsal olaylardan etkilenerek yaşayan canlı bir varlıktır. Toplumu ilgilendiren ciddi konulardaki olayların dil üzerinde etkisinden söz etmek olasıdır. Konu kapsamında ele alındığında savunma sanayii alanındaki gelişmeler, dile yeni kavramların girmesine zemin hazırlamıştır. İlk olarak "Mavi Vatan" olarak üretilen bu söz öbeği "Gök Vatan" ve "Siber Vatan" ifadelerinin kavramlaşmasına zemin oluşturmuştur. Nitekim bu kavramların yerleşikliği, devletin öncelik ve önem verdiği güvenlik politikalarının da bir göstergesi olarak yorumlanabilir. Bu yaklaşımla Aydın tarafından (Aydın, 2022) *siber vatan* kavramı, "Türkiye'nin dijital araçları ve kurumsal İnternet alanındaki altyapısını koruma doktrininin adı." olarak açıklanmaktadır.

Türkiye özelinde kamu kurumlarının çeşitlenerek kurulması ve hem lise hem de üniversitelerde uzmanlık düzeyinde bölümlerin açılmasıyla akademik ve teknik çalışmaların nicelik ve niteliklerinde artışlar olmaktadır. Farklı alanlarda kurumlarının açılması, konunun ciddiyetinin ve hassasiyetinin devlet politikası olarak etkin varlık gösterdiğine yönelik yorumlanabilir. Nitekim 2018 yılında kurulan ve kamusal olarak siber güvenlik faaliyetlerinin sorumlusu olarak kapsayıcı yetki alanına sahip Dijital Dönüşüm Ofisi (DDO) (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı, 2024), doğrudan Cumhurbaşkanlığına bağlı bir başkanlıktır. DDO, Türkiye'de ilk olarak kurulan Siber Güvenlik Meslek Yüksekokullarının kuruculuğunu üstlenmiştir. Bununla birlikte DDO, Türkiye'nin ilk siber güvenlik lisesi Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesinin de kurucu unsurları arasındadır. Ayrıca, Dijital Dönüşüm Ofisi tarafından Milli Eğitim Bakanlığı iş birliğiyle ilkokul, ortaokul ve lise öğrencilerine yönelik "Siber Zeka Bilgi Yarışması" (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı, 2020) 2020'den bu yana düzenlenmektedir.

Siber güvenlik alanındaki nitelikli insan gücünün yetiştirilmesi çalışmalarında SSB bünyesinde faaliyet gösteren Türkiye Siber Güvenlik Kümelenmesinden (Siber Küme) söz edilebilir. 2018 yılında kurulan Siber Küme, çevrim içi ve yüz yüze olarak gerçekleştirdiği öğretim faaliyetleriyle sektörel iş birliklerini artırmakla birlikte lise ve üniversite öğrencilerine yönelik yaz kampı, kış kampı ve gece eğitim programları sunmaktadır. Bunların yanı sıra Siber Küme de Teknopark İstanbul MTAL'nin

paydaşları arasındadır. Bu çalışmanın kapsamı gereği Siber Küme'nin iki hedefine (Türkiye Siber Güvenlik Kümelenmesi, 2024) burada yer verilebilir: *1) Siber güvenlik alanındaki insan kaynağı sayısı ve niteliğini arttırmak. 2) Toplumdaki siber güvenlik bilincini arttırmak*.

TRT Çocuk ve Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı ortaklığıyla çocuklara yönelik hazırlanan ve 14 Mayıs 2022 tarihinde yayınlanan "Ekip: SİBERAY" (Siber Suçlarla Mücadele Daire Başkanlığı, 2020) çizgi filmi dizisi aynı zamanda sinema filmi olarak 5 Nisan 2024'te vizyona girmiştir.

Yukarıdaki ifadelerin yanı sıra bu alt başlıkta, Cumhurbaşkanlığı ve Bakanlık düzeyinde yayınlanan ilgili belgeler doğrultusunda Türkiye'nin siber güvenlik alanındaki nitelikli iş gücü politikasına genel bir bakış ortaya konacaktır. Söz konusu belgelerde yer alan stratejik ifadeler, aynı zamanda ele alınan bu dönem projesinin bir tür dayanağı ve çıktısı olarak değerlendirilebilir. Ayrıca, küresel anlamda bir sorun olan nitelikli siber güvenlik uzmanı yetiştirilmesine yönelik Türk devletinin en üst düzeyde işaret ettiği etkin politikasını göstermesi açısından da önem arz etmektedir.

Güncel olarak iki belgenin varlığı görülmektedir. Resmi olarak belirtilen adlarıyla:

1. 2024 Yılı Cumhurbaşkanlığı Yıllık Programı (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023)
2. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020)

2024 Yılı Cumhurbaşkanlığı Yıllık Programı'nda siber güvenlik öğretimi ve alan üzerine nitelikli iş gücünün yetiştirilmesine yönelik eylem planlarının yer aldığı görülmektedir.

- *Tedbir 521.4* olarak yer verilen "Gerek savunma ve güvenlik gerekse sivil alanda siber güvenlik ihtiyaçları, azami ölçüde yerli ve yetkin çözümlerle karşılanacaktır." ile *Kalkınma Planı p.582*'de "Yerli siber güvenlik ekosisteminin gelişmesi, milli çözümlerin yaygınlaşması ve uluslararası rekabet gücünün artırılması sağlanacaktır." (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023) yaklaşımları önemlidir. Nitekim siber güvenlik öğretimi üzerine yabancı çözümler yaygın olarak kullanılmaktadır.
- Cumhurbaşkanlığı Yıllık Programı'nda *Kalkınma Planı p.452*, *Kalkınma Planı p.557* ve *Kalkınma Planı p.583* başlıklarında (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023) yapay zeka ve siber güvenliğin de yer aldığı güncel teknolojilerin ihtiyaç duyduğu altyapıların tesis edilmesi ve ihtiyaç duyulan nitelikli insan kaynağının yetiştirilmesine vurgu yapılmaktadır.

Siber güvenlik, ekonomik boyutunun yanı sıra ulusal güvenlikle yakından ilgilidir. Bu yönüyle kritik bir öneme sahip olduğu Cumhurbaşkanlığı Yıllık Programı'nda da yinelenmektedir.

- *Tedbir 583.1'*de (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023) "Siber güvenlik alanında nitelikli işgücünün yetiştirilmesine ve kariyer

olanaklarının iyileştirilmesine yönelik programlar geliştirilecektir." ifadesinde alt ifade olarak "Nitelikli genç istihdama yönelik siber güvenlik yarışmaları düzenlenecektir." denilmektedir.

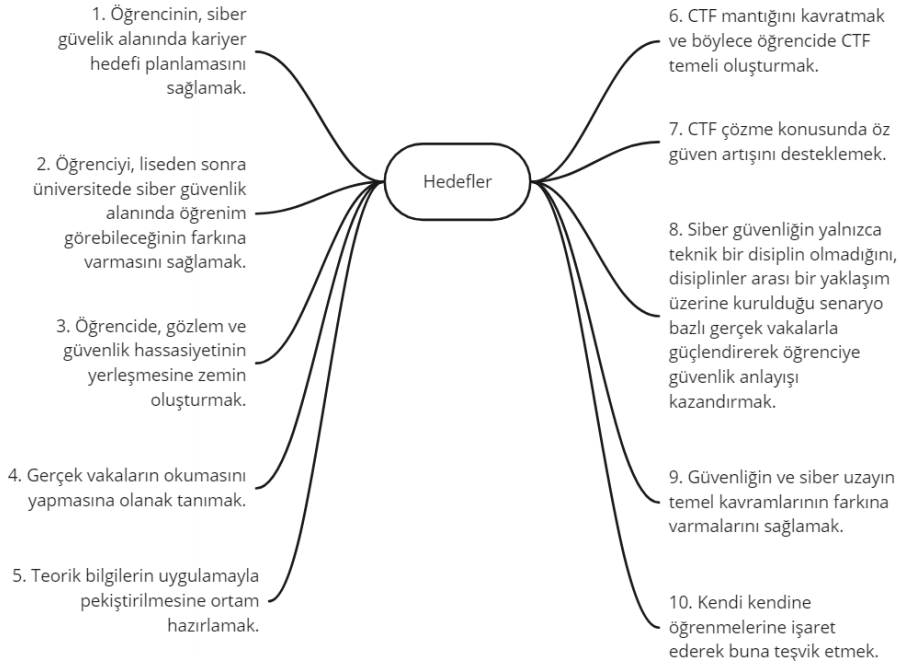
- *Tedbir 583.3*'te (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023) "Sektör ihtiyaçlarına uygun işgücünün yetiştirilmesi amacıyla eğitim içerikleri, niteliği ve ortamı geliştirilecektir." ifadesinin altında "Çevrim içi ve laboratuvar ortamında siber güvenlik eğitimleri gerçekleştirilecektir." hedefi de siber güvenlik yarışmalarının süreçte etkin yer almasına işaret etmektedir.
- *Tedbir 583.4*'te (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023) "Siber güvenlik farkındalığına yönelik seminer, eğitim, yarışma gibi etkinlikler gerçekleştirilecektir." ve "İlk ve ortaöğretim seviyesinde siber güvenliğe yönelik ders içeriğinin geliştirilmesi çalışmaları yapılacaktır." hedefleri yetkin siber güvenlik profesyonellerinin örgün müfredat aracılığıyla yetiştirilmesine yöneliktir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) belgesinde (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020) nitelikli iş gücünün yetiştirilmesine yönelik "Süreçlerin iyileştirilmesi, teknolojik bileşenlerden azami seviyede istifade edilmesi ve insan kaynağının geliştirilmesine yönelik eylemlerle siber güvenlik seviyesinin daha da yükseltilmesi amaçlanmıştır." ifadeleri bulunmaktadır. Yanı sıra ilgili belgede "İlk ve orta dereceli okullar ile yükseköğrenimde siber güvenlik eğitim içeriklerinin zenginleştirilmesi ve yaygınlaştırılmasını hedef alan eylemlerle bu alandaki insan kaynağının artırılması amaçlanmıştır." yine bu çalışmanın kapsamında değerli ifadelerdir. İlgili belgenin *Ulusal Siber Güvenlik Hedeflerimiz* başlığında geçen şu ifadeler dikkat çekicidir: "Siber güvenliğe ilgi duyan veya uzmanlaşmak isteyen bireylere yönelik projelerle insan kaynağının güçlendirilmesi.".

3. ÖNERİLEN EĞİTİM SİSTEMİ YAKLAŞIMI

Ele alınan çalışmanın işe yararlılığını ortaya koymak ve disiplinli bir biçimde konuları ele alabilmenin yolunun, öncelikli olarak söz konusu projenin hedeflerinin açık biçimde yazılmasından geçtiğini düşünmekteyiz. Bu başlık altında önerilen eğitim sisteminin hedefleri ve gerçekleştiğinde öğrencinin edineceği öngörülen kazanımlar açıklanacaktır.

Bayrak Sende adında bir platform üzerinde kurgulanan tüm senaryo ve soruların, amacına bütünüyle hizmet edebilmesi için Şekil 2'de belirtilen hedeflerle uyumlu olmasına özen gösterilmesi beklenmektedir.



Şekil 2. Önerilen Eğitim Sistemi Yaklaşımı

1. hedef: *Öğrencinin, siber güvelik alanında kariyer hedefi planlamasını sağlamak.*

Kazanımı: Teknolojik cihazların toplum geneline yaygınlaşmasıyla İnternet'e bağlanan bu cihazlar, siber uzaydaki varlıkların sayısında devasa artışlara yol açmaktadır. Bu genişlemenin bir sonucu olarak söz konusu varlıklara yönelik tehditlerin artması doğru bir korelasyon göstermektedir. Bu noktada toplumsal bir siber güvenlik bilincinin gerekliliği konuşulurken alan üzerine profesyonellerin eğitimi de dünya genelinde gündemde olan bir konudur. Tıpkı sağlıklı biçimde istihbarat ve güvenlik algısının toplumda yaygınlaşmasıyla oluşacak bilinçteki katkılarında olduğu gibi siber güvenlikte de kamusal bilincin benimsenmesi güvenliğin temel çatısından ayrı görülmemelidir. Siber güvenilir bir toplum ancak böylesi bir yaygın bilinçlenmeden geçmektedir. Siber Vatan'ın direnci nitelikli insan gücünün varlığıyla olasıdır.

Siber güvenlikte nitelikli iş gücünün oluşturulması ve var olan potansiyelin güçlendirilmesi, toplumda siber güvenliğin bir kariyer yolu olarak görülmesiyle doğrudan bağlantılıdır.

Caroline Rose Ster, doktora tezinde (Ster, 2019) siber güvenlikte uzman eksikliğinin nedenlerinden biri olarak siber güvenliğin bir kariyer planı olarak değerlendirilebileceğinin farkında olunmamasına bağlamaktadır. Yazar, düzenlenen siber güvenlik etkinliklerini uygun bir halkla ilişkiler çalışmalarıyla desteklenmesini bu yüzden önemsemektedir. Ster, halkla ilişkiler çalışmasında yalnızca öğrencileri değil ailelerini de hedeflediklerini ifade etmektedir çünkü siber güvenliğin bir kariyer planına dahil edilebilmesinde ebeveynlerin de etkisinin olduğunu düşünmektedir. Yazar, anne-

babaların siber güvenlik alanında bir gelecek görürlerse çocuklarını da bu gibi etkinliklere katılmalarında teşvik edici olacaklarını ifade etmektedir. Elbette, *Bayrak Sende* platformunun amacı doğrudan ailelere yönelik değildir. Bu ifadelere yer verilmesindeki amaç, siber güvenlikte kariyer planlaması yapılmak istendiğinde bunun yalnızca öğrenciyle sınırlı olmadığını vurgulamaktır.

Türkiye'de olduğu gibi yurt dışında da nitelikli üniversitelerden kabul almanın daha rekabetçi bir hale geldiği yapılan araştırmalarda (Ster, 2019) dile getirilmektedir. Liseye geçiş sınavında da benzer bir zorluğun olduğu bilinmektedir. Bu rekabet daha ortaokulda başlamaktadır. Öğrencinin, liseye giriş sınavında iyi bir sıralamaya girmek ve yüksek puan alabilmek adına ilgi duyduğu sanatsal ve/veya bilimsel faaliyetlerden geri durmak zorunda kalmaktadır.

Ortaokul yıllarının ardından liseye geçen öğrenci, ortaokuldaki gibi üniversite sınavına yoğunlaşmadan önce siber güvenlik alanındaki ilgisini kariyere yönlendirmek bu açıdan bir zaman aralığı tanıyabilmektedir. Böylesi bir sınav maratonunda ders dışı etkinliklerde heveslendirici ve heyecan uyandırıcı faaliyetlerin önemi ve katkısı yüksek olmaktadır. Ortaokul ve lise yıllarında siber güvenlik faaliyetleri içerisinde olan öğrenci, bir sonraki eğitim düzeyine geçeceğinde bu alanı deneyimlemiş olduğundan karar vermede daha isabetli ve sürdürülebilir bir sonuca ulaşabilir.

White ve ark. (White, Williams, & Harrison, 2010) siber güvenliğe olan hazırlığın üniversiteden önce başlatılmasını ifade ettikleri çalışmalarında, ABD'de uygulanan "Cyber Patriot"ı incelemektedirler. Çünkü lise düzeyindeki öğrencilerin kariyer planlamada henüz yolun başında ve ilgi alanlarını keşfetme sürecinde oldukları için lise öğrencilerine yönelik faaliyetlere dikkat çekmektedirler.

ABD'de siber güvenlik alanında çalışacak nitelikli iş gücünün oluşturulması ve geliştirilmesi güvenlik teşkilatlarının da sorumluluk alanında değerlendirilmektedir. Öyle ki ABD Siber Komutanlığı, Ulusal Güvenlik Ajansı ve İç Güvenlik Bakanlığının bu yönde etkin yer aldığı görülmektedir. Üniversitelerle iş birliği içerisinde olan bu devlet kurumları (White, Williams, & Harrison, 2010) siber güvenlik yarışmaları düzenlemektedirler. Yapılan akademik çalışmalarla desteklenmektedir ki BYY gibi siber güvenlik yarışmalarının öğrencilere siber güvenlik alanında ufuklar açtığı ve kariyer olasılıklarını sunma konusunda başarılıdır. Carnegie Mellon Üniversitesinin siber güvenlik programları ve çalışmaları doğrudan NSA ve DHS tarafından desteklenmekte ve ilgili web sayfasında (Carnegie Mellon University CyLab, 2024) açıkça belirtilmektedir. ABD'deki siber güvenlik faaliyetlerinde kamu kurumlarının etkin bir yapılanma ve iş birliği içinde olduğu görülmektedir. ABD'nin etkin istihbarat servislerinden olan ve Savunma Bakanlığına bağlı olarak faaliyet gösteren NSA bu konuda, çocuklar ve gençler arasında siber güvenliğe olan ilginin artırılması noktasında görev üstlenmektedir. Ulusal Bilim Vakfı ile destekledikleri GenCyber projesi, doğrudan K-12 düzeyindeki öğrencilere odaklıdır.

2022 yılında ABD'de yapılan bir araştırmada liseden mezun olanların %75'inin üniversite seçiminde ve kariyer planlamada karar vermeye yeterince hazırlıklı olmadıkları ifade edilmektedir. Öğrenciler, iş hayatına atılmada kendilerini yeterli görmediklerini düşündüklerini belirtmektedir (Wagner, 2023).

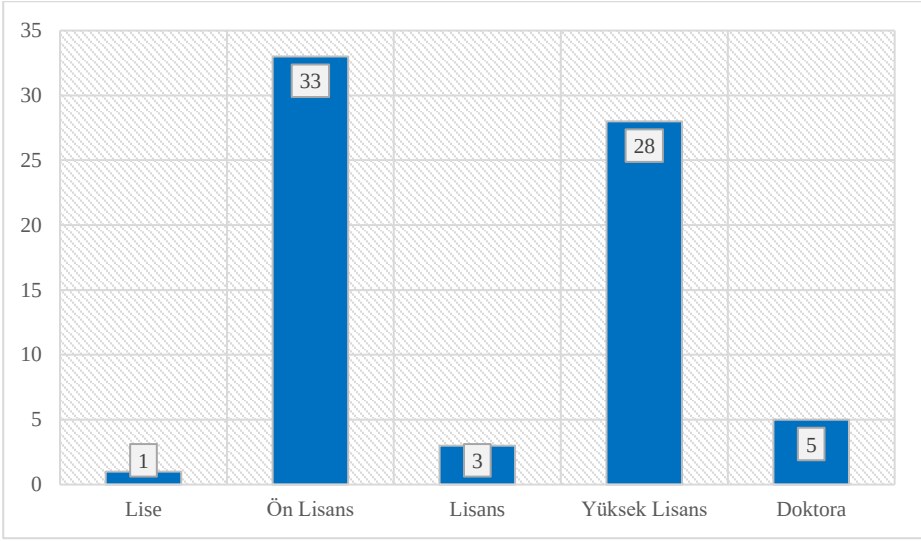
2021 yılına ait bir araştırmada Avrupa ve ABD'nin siber güvenlik iş gücünde %30'luk bir artış olduğu kaydedilse de siber güvenlik uzmanlarına yönelik küresel ihtiyaçtaki mevcuttaki iş gücüne kıyasla makasın açıldığına dikkat çekilmektedir. Ülkenin maruz kaldığı ve kalacağı siber ataklara karşı savunmanın ön cephesini oluşturan yetkin siber güvenlik personelinin hazırbulunuşluğunu zorunlu kılmaktadır. Bu hazırbulunuşluğun desteklenmesi ve kapasitenin artırılması için de şirketler ve kurumlar hizmet içi eğitim ve öğretimle buna katkı sağlayabilir. Yunanistan'da yapılan bir çalışmada (Katsantonis ve ark., 2023) bu endişelere yer verilmektedir.

Microsoft'tan Lewis Shepherd'ın (White ve ark., 2010) yetenekli siber güvenlik personellerine olan ihtiyacın, yetiştirilen öğrencilerin çok ötesinde olduğunu ifade etmesi ve bunun ABD başta olmak üzere diğer ülkelerdeki eğitim sistemlerinin yetersiz kalmasına değinmesi önemli bir ayrıntıdır. Yanı sıra MITRE'den Cherinka ve Prezzama'nın (Cherinka & Prezzama, 2015) da dikkat çektiği üzere kariyerinin başındaki birey, kendince tecrübeli olan meslektaşlarına göre daha yenilikçi ve heyecan verici fikirlerle atılım gösterme eğilimindedirler.

2. hedef: *Öğrenciyi, liseden sonra üniversitede siber güvenlik alanında öğrenim görebileceğinin farkına varmasını sağlamak.*

Kazanımı: Öğrencilerin, liseden mezun olduklarında üniversite kariyerlerine doğrudan siber güvenlikte devam etmeleri mümkündür.

Dijital Dönüşüm Ofisi öncülüğünde kurularak 2023-2024 yılında eğitim ve öğretime başlayan Siber Güvenlik Meslek Yüksekokulları bulunmaktadır (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı, 2023). Yükseköğretim Kurulunun Ön Lisans Atlası'ndan edinilen bilgiler doğrultusunda Siber Güvenlik MYO'larına ek olarak ön lisans düzeyinde "Siber Güvenlik", "Bilişim Güvenliği Teknolojisi" adlarıyla tercih edilebilirler. Lisans olarak "Adli Bilişim Mühendisliği" ve "Bilgi Güvenliği Teknolojisi" adıyla iki bölüm bulunmaktadır (Yükseköğretim Kurulu, 2024). Lisansüstü düzeyinde ise vakıf ve devlet üniversitelerinde yüksek lisans ve doktora eğitimleri oldukça çeşitlidir. Türkiye'de siber güvenlik alanında eğitim ve öğretim programı uygulayan okulların sınıflandırması ve sayısı Şekil 3'te verilmektedir.



Şekil 3. Türkiye Özelinde Siber Güvenlik Alanında Eğitim Veren Okul Sayısı

3. hedef: *Öğrencide, gözlem ve güvenlik hassasiyetinin yerleşmesine zemin oluşturmak.*

Kazanımı: Kurgulanacak senaryolarda ve hazırlanacak sorularda yalnızca bilgisayar bilimlerinde yetkinlik oluşturmak/geliştirmekle yetinilmemesi önerilmektedir. Nitekim siber güvenlik bir bütün olarak ele alınması gereken bir disiplindir. Söz öbeğinin başında "siber" olması, peşi sıra gelen "güvenlik" ifadesinin dışında tutulmamalıdır. Bu araştırma çalışmasında ayrıca değinildiği üzere siber güvenlik, ulusal güvenlikten bağımsız değildir. Buradan hareketle senaryo ve soruların içeriğinde öğrencinin gözlem ve güvenlik hassasiyetinin oluşmasına/geliştirilmesine katkı sağlayacak bir yaklaşım ortaya konulmalıdır.

4. hedef: *Gerçek vakaların okumasını yapmasına olanak tanımak.*

Kazanımı: Bayrak Sende'de ortaya konan her bir görev olabildiğince yaşanmış vakalarla desteklenmelidir. Bu kazanım, özellikle öğrencinin teorik ya da uygulamalı gördüğü derslerde öğretmenine yönelttiği "Bu bilgiler gerçek hayatta ne işime yarayacak?" sorgulamasını besleyen bir yöne sahiptir. Örneğin, seyahat güvenliği üzerine bir görevdeki sorunları çözmeye çalıştığında bunun öylesine yazılmak için ele alınan bir soru olmadığının farkına varabilecektir çünkü seyahat güvenliği dikkate alınmadığında üst düzey görevlilerin kriptolu cihazlarına bile sızılabildiğini açık kaynaklara yansıyan siber espiyonaj faaliyetiyle görebilir olacaktır.

5. hedef: *Teorik bilgilerin uygulamayla pekiştirilmesine ortam hazırlamak.*

Kazanımı: Uygulama yapmak, etkili bir öğrenme yöntemidir. Siber güvenlik çözümlerinde tek bir çözüm yönteminin olmayışı ona bir açık uçlu sorulardaki gibi yanıt verirken özgür bir ifade ortamı sunabilmektedir. Bu da öğrencinin bağımsız

düşünebilmesi gibi bilişsel becerilerini kullanmasına zemin bırakır (Rowe, Lunt, & Ekstrom, 2011). Öğrenimin pekiştirilmesi adına uygulamalı laboratuvarların kullanımının üretkenliği ve etki düzeyini arttırdığı bilinmektedir (Son, Irrechukwu, & Fitzgibbons, 2012). Pedagojik uygulama alanlarından biri olan bu yöntem eğitim bilimlerinde sıkça vurgulanan Howard Gardner'ın "Çoklu Zeka Kuramı"nda da bulunmaktadır.

6. hedef: *BYY mantığını kavratmak ve böylece öğrencide BYY temeli oluşturmak.*

Kazanımı: Öğrenimin varacağı nihai nokta öğrencisine bayrağı yakalatmaktır. Öğrenci, Bayrak Sende'deki görevleri tamamladıkça bir BYY'nin ne olduğunu, katılımcısından neler beklediğini, BYY'deki sorulara nasıl yaklaşılması gerektiği noktalarında bir kavrayış oluşturulması hedeflenmektedir.

7. hedef: *BYY çözme konusunda öz güven artışını desteklemek.*

Kazanımı: Bayrak Sende'deki görevler, öğreticilik sağlarken BYY'lerdeki mantığı temele alarak soruları öğrenciye yöneltir. Böylelikle öğrenci, platformu etkin kullandıkça BYY'leri çözerek eleştirel bakış kazanabilecek, problem çözme becerilerini geliştirebilecek ve bir sonraki aşamalarda ulusal ve uluslararası BYY'lere katılmada öz güvenini güçlendirebilecektir. Öz güvenin olması kişisel hayatında da etki sağlayabileceği gibi teknik olarak da daha ileri öğrenmeler ve gelişimler için sağlam bir temel olacaktır.

8. hedef: *Siber güvenliğin yalnızca teknik bir disiplin olmadığını, disiplinler arası bir yaklaşım üzerine kurulduğu senaryo bazlı gerçek vakalarla güçlendirerek öğrenciye güvenlik anlayışı kazandırmak.*

Kazanımı: Siber uzayın, ulusal güvenlikle ilişkisine yönelik yaklaşımlar "Ulusal Güvenlik Bağlamında Siber Uzay" bağlığında ortaya konmaya çalışılmıştı. Bu bilgiler doğrultusunda öğrenciye gerçek hayatta yaşanan vakalar üzerinden senaryolar sunularak öğrendiği/öğreneceği bilgilerin nerelerde hangi amaçlar nasıl kullanılacağı noktasında bir bakış kazandırılması önceliklendirilmektedir.

9. hedef: *Güvenliğin ve siber uzayın temel kavramlarının farkına varmalarını sağlamak.*

Kazanımı: Temel kavramlar çoğunlukla basit ve geçiştirilecek konular gibi algılanır. Ne ki, bu yaygın kanının aksine yeni başlayan birisi için temel kavramların doğru biçimde edinilmesi sonraki öğrenme aşamasında sağlıklı bir zemin hazırlar. Temel kavramları öğretmek yalnızca terim açıklamalarını retorik olarak ele almak olarak değerlendirilmemelidir. Bu hedefle birlikte öğrenciye sağlam bir temel oluşturulması amaçlanmaktadır. Böylece, sağlam zemin üzerine inşa edilecek bina öğrencinin kendi çabasıyla mümkün olabilecektir.

10. hedef: *Kendi kendine öğrenmelerine işaret ederek buna teşvik etmek.*

Kazanımı: Siber güvenlik alanı sürekli öğrenimi gerektiren bir yapıya sahiptir. Konu çeşitliliği, derinliği ve hareketliliği yönleriyle tıp bilimiyle benzerlik göstermektedir.

Bu doğrultuda öğrencisinden ömür boyu öğrenci kalabilmeyi bekler. Bayrak Sende'deki iletişim yaklaşımı ve görevlerdeki içerikler de bu kapsamda ele alınabilmelidir. Öğrenmeyi öğrenen bir öğrenci, öz disiplinini edinebildiğinde öz motifini bularak kendi hedefleri doğrultusunda kararlı bir ilerleme ortaya koyabilecektir.

6. SONUÇ

Siber uzay geleneksel harp sahaları olan kara, deniz, hava ve uzaydan sonra beşinci saha olarak güvenlik literatüründeki yerini almıştır. Siber güvenlik gibi çok yönlü bir disipline sahip alandaki nitelikli profesyonel eksikliği ise gerek özel sektörde gerek kamuda ciddi güvenlik sorunlarına neden olmaktadır. Bilişim teknolojilerinin toplumun her alanına girmesi, devletin kritik altyapılarının ve varlıkların dijitalleşmesi gibi gelişmeler siber uzayı ulusal güvenliğin merkez noktasına taşımaktadır. Bu noktada ülkeler, siber güvenlikte yetkin insan gücünü eğitmek, geliştirmek ve istihdam etmek adına çeşitli faaliyetler ortaya koymaktadır. Bunlardan biri de bayrağı yakala yarışmalarıdır. Bu çalışmada, siber güvenlik alanında istihdam edilecek nitelikli iş gücünün yetiştirilmesinde bir eğitim yaklaşımı olarak bayrağı yakala yarışmalarının geçerliği üzerinde durularak bir yaklaşım sunmaya çalışılmış olup bir öğretim modeli hedefler ve kazanımlarıyla aktarılmıştır.

Yazarların Katkısı
Yazarların makaleye katkıları eşit orandadır. Bu çalışmada Cafer ULUÇ fikir, araştırma, kaynak taraması, değerlendirme, analiz, bilgisayar ortamında testlerin gerçekleştirilmesi ve makalenin yazımı konusunda katkıda bulunmuştur. Can EYÜPOĞLU fikir, eleştiri, danışmanlık, yazım dili, araştırma, kaynak taraması, makalenin yazımı ve değerlendirilmesi konusunda katkı sağlamıştır.

Teşekkür
Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi öğrencilerine araştırma boyunca sağladıkları destekten dolayı teşekkür ederiz.

Çıkar Çatışması Beyanı
Yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır.

Araştırma ve Yayın Etiği Beyanı
Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

KAYNAKÇA

Albert, R. T., & Wallingford, J. L. (2010). Cyber Defense Competitions-Educating for Prevention. *Proceedings of the 2010 ASCUE Summer Conference*, (s. 22-30). North Myrtle Beach, SC, USA.

Aydın, E. (2022). Mavi Vatan, Gök Vatan ile Siber Vatan Söz Öbeklerinin Anlamları ve Oluşturulma Yöntemleri. *The Journal of Turkic Language and Literature Surveys (TULLIS)*, s. 168-178.

California Cybersecurity Institute. (2024). *Our Supporters*. https://cci.calpoly.edu/about-cci/our-supporters adresinden 29 Şubat 2024 tarihinde alındı.

Canadian Centre for Cyber Security. (2022). *An Introduction to the Cyber Threat Environment (2023-2024).* Ottawa: Canadian Centre for Cyber Security. https://www.cyber.gc.ca/sites/default/files/ncta-2022-intro-e.pdf adresinden 17 Şubat 2024 tarihinde alındı.

Carnegie Mellon University CyLab. (2024). *Education*. https://www.cylab.cmu.edu/education/index.html adresinden 29 Şubat 2024 tarihinde alındı.

Chase, J. D., & Uppuluri, P. (2022). High School Cybersecurity? Challenge Accepted – Radford University's RUSecure CTF Contest for High School Students. *Journal of The Colloquium for Information Systems Security Education,* 9(1), s. 1-6.

Cherinka, R., & Prezzama, J. (2015). Innovative Approaches to Building Comprehensive Talent Pipelines: Helping to Grow a Strong and Diverse Professional Workforce. *Systemics, Cybernetics and Informatics, 13*(6), s. 82-86.

Chou, T.-S., & Jones, J. (2018). Developing and Evaluating an Experimental Learning Environment for Cyber Security Education. *SIGITE '18: Proceedings of the 19th Annual SIG Conference on Information Technology Education*, (s. 92-97). Fort Lauderdale, FL, USA.

Chung, K. (2017). Lowering the Barriers to Capture The Flag Administration and Participation. *USENIX Workshop on Advances in Security Education.* Vancouver, BC, Canada.

Chung, K., & Cohen, J. (2014). Learning Obstacles in the Capture The Flag Model. *USENIX Summit on Gaming, Games, and Gamification in Security Education.* San Diego, CA, USA.

Conti, G., Babbitt, T., & Nelson, J. (2011, 5 23). Hacking Competitions and Their Untapped Potential for Security Education. *IEEE Security & Privacy*, s. 56-59.

Cooper, T. T., & Harris, J. T. (2022). Cyber Red Zone: Capture-the-Flag the DoD Way! *MODSIM World 2022: Building a Better Tomorrow.* Norfolk, VA, USA.

Cusak, A. (2023). Case Study: The Impact of Emerging Technologies on Cybersecurity Education and Workforces. *Journal of Cybersecurity Education, Research and Practice*, s. 1-12.

Cyber Patriot. (2024). *Elementary School Cyber Education Initiative*. https://www.uscyberpatriot.org/Pages/Special%20Initiatives/Elementary-School-Initiative.aspx adresinden 24 Şubat 2024 tarihinde alındı.

Cyber Patriot. (2024). *Sponsors*. https://www.uscyberpatriot.org/Pages/About/Sponsors.aspx adresinden 24 Şubat 2024 tarihinde alındı.

Cyber Patriot. (2024). *What is Cyber Patriot?* https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx adresinden 24 Şubat 2024 tarihinde alındı.

Cybersecurity and Infrastructure Security Agency. (2024). *Cybersecurity Awareness Month*. https://www.cisa.gov/cybersecurity-awareness-month adresinden 27 Şubat 2024 tarihinde alındı.

Davis, A., Leek, T., Zhivich, M., Gwinnup, K., & Leonard, W. (2014). The Fun and Future of CTF. *USENIX Summit on Gaming, Games, and Gamification in Security Education.* San Diego, CA, USA.

Defense News. (2024). *Top 100 Defense Companies*. https://people.defensenews.com/top-100/ adresinden 29 Mart 2024 tarihinde alındı.

Dill, K. J. (2018). Cybersecurity for the Nation: Workforce Development. *The Cyber Defense Review*, s. 55-64.

Eagle, C., & Clark, J. L. (2004). Capture-the-Flag: Learning Computer Security Under Fire. *Proceedings from the Sixth Workshop on Education in Computer Security (WECS6)*, (s. 18-21). Monterey, CA, USA.

Ford, V., Siraj, A., Haynes, A., & Brown, E. (2017). Capture the Flag Unplugged: An Offline Cyber Competition. *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*, (s. 225-230). Seattle Washington, USA.

Government of the United Kingdom. (2015, 11 21). *National Security Strategy and Strategic Defence and Security Review 2015*. https://assets.publishing.service.gov.uk/media/5a74c796ed915d502d6caefc/52309_Cm_9161_NSS_SD_Review_web_only.pdf adresinden 1 Mart 2024 tarihinde alındı.

Haggman, A. (2019). *Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education.* London, UK: Royal Holloway, University of London.

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training are Serious Games Suitable for Cybersecurity Training? *International Journal of Serious Games*, s. 53-61.

Katsantonis, M. N., Manikas, A., Mavridis, I., & Gritzalis, D. (2023). Cyber Range Design Framework for Cyber Security Education and Training. *International Journal of Information Security*, 3(18), s. 1005-1027.

Katzcy Consulting. (2016). *Cybersecurity Games: Building Tomorrow's Workforce.*

Küçükçekmece İlçe Milli Eğitim Müdürlüğü. (2016). *Liseler Arası Bilişim Kampı*. https://kucukcekmece.meb.gov.tr/www/liseler-arasi-bilisim-kampi/icerik/708 adresinden 5 Mart 2024 tarihinde alındı.

Langner, G., Andriessen, J., Quirchmayr, G., Furnell, S., Scarano, V., & Tokola, T. J. (2021). Poster: The Need for a Collaborative Approach to Cyber Security Education. *IEEE European Symposium on Security and Privacy (EuroS&P)*, (s. 719-721). Vienna, Austria.

LeClair, J., Abraham, S., & Shih, L. (2013). An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. *Information Security Curriculum Development Conference*, (s. 71-78). Kennesaw, GA, USA.

Leune, K., & Petrilli, S. J. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. *SIGITE '17: Proceedings of the 18th Annual Conference on Information Technology Education*, (s. 47-52). New York, NY, USA.

Li, C., & Kulkarni, R. (2016). Survey of Cybersecurity Education through Gamification. *ASEE's 123rd Annual Conference & Exposition.* News Orleans, LA, USA.

Manson, D., Curl, S., & Carlin, A. (2012). CyberPatriot: Exploring University-High School Partnerships. *Communications of the IIMA*, s. 65-77.

Matias, P., Barbosa, P., Cardoso, T. N., Campos, D. M., & Aranha, D. F. (2018, 12). NIZKCTF: A Noninteractive Zero-Knowledge Capture-the-Flag Platform. *IEEE Security & Privacy, 16*(6), s. 42-51.

McGoogan, C. (2015, 10 1). *Want to be a GCHQ spy? Play this game*. https://www.wired.co.uk/article/cyphinx-cybersecurity-game adresinden 29 Şubat 2024 tarihinde alındı.

Milli İstihbarat Teşkilatı. (2024). *2023 Yılı Faaliyet Raporu.* Ankara. https://mit.gov.tr/uploads/f/znyYgMZdUvDr.PDF adresinden 29 Şubat 2024 tarihinde alındı.

Milli İstihbarat Teşkilatı. (2024). *İstihbarat Sözlüğü*. 2 https://www.mit.gov.tr/sozluk.html adresinden 3 Şubat 2024 tarihinde alındı.

National Initiative for Cybersecurity Education. (2024). *Events*. https://niceconference.org/events/ adresinden 20 Şubat 2024 tarihinde alındı.

Noor Azam, M., & Beuran, R. (2018). *Usability Evaluation of Open Source and Online Capture the Flag Platforms.* Nomi, Ishikawa, Japan: Japan Advanced Institute of Science and Technology (JAIST).

Raman, R., Sunny, S., Pavithran, V., & Achuthan, K. (2014). Framework for Evaluating Capture the Flag (CTF) Security Competitions. *IEEE International Conference for Convergence of Technology*, (s. 1-5). Pune, India.

,

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The Role of Cyber-Security in Information Technology Education. *SIGITE '11: Proceedings of the 2011 Conference on Information Technology Education*, (s. 113-121). West Point, NY, USA.

Siber Suçlarla Mücadele Daire Başkanlığı. (2020). *TRT Çocuk'ta "Ekip: SİBERAY"*. https://www.siberay.com/trt-cocuk-ekranlarinda-ekip-siberay adresinden 10 Nisan 2024 tarihinde alındı.

Son, J., Irrechukwu, C., & Fitzgibbons, P. (2012). Virtual Lab for Online Cyber Security Education. *Communications of the IIMA, 12*(4), s. 81-101.

Ster, C. R. (2019). *Engaging High School Students Towards a Career in Cybersecurity.* San Luis Obispo, CA, USA: California Polytechnic State University.

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2020, 12 27). Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges. *Computers & Security*, s. 1-14.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı. (2020, 10 20). *Siber Zeka Bilgi Yarışması*. https://cbddo.gov.tr/haberler/4906/siber-zeka-bilgi-yarismasi adresinden 24 Şubat 2024 tarihinde alındı.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı. (2023, 7 31). *Siber Güvenlik Meslek Yüksekokulları*. https://cbddo.gov.tr/sss/siber-myo/ adresinden 4 Mart 2024 tarihinde alındı.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı. (2024). *Hakkımızda*. https://cbddo.gov.tr/hakkimizda/ adresinden 8 Mart 2024 tarihinde alındı.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2023). *2024 Yılı Cumhurbaşkanlığı Yıllık Programı.* Ankara.

T.C. Milli Savunma Bakanlığı. (2023). *Kilitli Kalkan-2023 (Locked Shields-2023) Tatbikatı Başarıyla İcra Edildi*. https://www.msb.gov.tr/Basin-ve-Yayin/Aciklamalar/985842bda91d49b7986792203ca5a602 adresinden 3 Mart 2024 tarihinde alındı.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.* Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023).* Ankara.

Tadjdeh, Y. (2013). Industry, Military Emphasize Need for Cyberwarrior Training as Attacks Increase. *National Defense*, s. 46-48.

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi. (2023). 2015'ten 2020'ye Okulumuzun Kuruluş Öyküsü. *Betik*(1), s. 48-53.

The Economist. (2010). *War in the Fifth Domain*. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain adresinden 23 Şubat 2024 tarihinde alındı.

The NATO Cooperative Cyber Defence Centre of Excellence. (2024). *Locked Shields*. https://ccdcoe.org/exercises/locked-shields/ adresinden 3 Mart 2024 tarihinde alındı.

Türkiye Siber Güvenlik Kümelenmesi. (2024). *Türkiye Siber Güvenlik Kümelenmesi*. https://www.siberkume.org.tr adresinden 24 Şubat 2024 tarihinde alındı.

Uluç, C. (2017). *Liseler Arası Bilişim Kampı: Teknik Liselerde Bilgi Güvenliği Eğitimi Üzerine.* İstanbul: Kutlu Yayınevi.

Ünal, A. Y. (2017, 1 19). *"Siber yıldız" Olmak için 26 Bin Kişi Yarışacak*. https://www.aa.com.tr/tr/bilim-teknoloji/siber-yildiz-olmak-icin-26-bin-kisi-yarisacak/730467 adresinden 5 Mart 2024 tarihinde alındı.

Ünal, A. Y. (2017, 1 19). *"Siber Yıldız" Olmak için 26 Bin Kişi Yarışacak*. https://www.aa.com.tr/tr/bilim-teknoloji/siber-yildiz-olmak-icin-26-bin-kisi-yarisacak/730467 adresinden 5 Mart 2024 tarihinde alındı.

Wagner, P. (2023). *CyberEducation-By-Design: Devoloping a Framework for Cybersecurity Education at Secondary Education Institutions in Arizona.* Dakota, SD, USA: Dakota State University.

Werther, J., Zhivich, M., Leek, T., & Zeldovich, N. (2011). Experiences in Cyber Security Education: The MIT Lincoln Laboratory Capture-the-Flag Exercise. *4th Workshop on Cyber Security Experimentation and Test (CSET 11).* San Francisco, CA, USA.

White, G. B., Williams, D., & Harrison, K. (2010). The CyberPatriot National High School Cyber Defense Competition. *IEEE Security & Privacy, 8*, s. 59-61.

Wi, S., Choi, J., & Cha, S. K. (2018). Git-based CTF: A Simple and Effective Approach to Organizing In-Course Attack-and-Defense Security Competition. *ASE '18: USENIX Advances in Security Education Workshop*, (s. 1-9). Baltimore, MD, USA.

Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and Preliminary Evaluation of a Cyber Security Requirements Education Game (SREG). *Information and Software Technology*, s. 179-200.

Yükseköğretim Kurulu. (2024). *Yükseköğretim Program Atlası*. https://yokatlas.yok.gov.tr/index.php adresinden 4 Mart 2024 tarihinde alındı.