

TÜRKİYE'DE "SİBER GÜVENLİK" EĞİTİMİNE DİSİPLİNLER ARASI BAKIŞ: MUHASEBE VE BANKACILIK BÖLÜMLERİ AÇISINDAN BİR ARAŞTIRMA¹

INTERDISCIPLINARY PERSPECTIVE ON "CYBER SECURITY" EDUCATION IN TURKEY: A RESEARCH IN TERMS OF ACCOUNTING AND BANKING DEPARTMENTS

Ayten ÖZBİNGÖL

Serbest Muhasebeci Mali Müşavir

Bağımsız Araştırmacı

aytenozbingol@gmail.com

ORCID: 0000-0002-6761-6569

ÖZ

ABSTRACT

Geliş Tarihi:

18.01.2025

Kabul Tarihi:

28.03.2025

Yayın Tarihi:

27.06.2025

Anahtar Kelimeler

Siber Güvenlik,
Siber Hukuk,
Muhasebe Eğitimi,
Bankacılık Eğitimi

Keywords

Cyber Security,
Cyber Security Law,
Accounting
Education,
Banking Education

Veri güvenliğine yönelik siber saldırı tehdidi, siber güvenliği önemli hâle getirmiştir. Bu nedenle, öncelikle Türkiye'deki 208 üniversitede "siber güvenlik" adı altında açılan, ön lisans, lisans ve lisansüstü eğitim programları incelenmiştir. Siber güvenlik eğitimlerinin mühendislik (fen bilimleri) alanında konumlandırıldığı belirlenmiştir. Siber güvenliğin disiplinler arası bir konu olması nedeniyle, bu çalışmanın amacı, sosyal bilimler alanında muhasebe ve bankacılık (lisans) eğitiminde siber güvenlik eğitiminin durumunu belirlemektir. Çalışmada içerik analizi yöntemi kullanılmıştır. Muhasebe alanında 15, bankacılık alanında 43 programın müfredatı siber güvenlik ve siber güvenlikle ilgili dersler açısından incelenmiştir. Muhasebe programlarının 6'sında, bankacılık programlarının 18'inde siber güvenlik ve siber güvenlikle ilişkili ders bulunmamaktadır. Muhasebe müfredatlarında "siber güvenlik" adı altında ders açan tek üniversite İstanbul Aydın Üniversitesi'dir. Bankacılık müfredatlarında "siber güvenlik" adı altında ders açan üniversiteler Erzincan Binali Yıldırım Üniversitesi ve İstanbul Nişantaşı Üniversitesi'dir. Siber güvenlikle ilişkili dersler açısından en zengin müfredat muhasebe programları arasında Başkent Üniversitesi'nde ve bankacılık programları arasında İstanbul Gelişim Üniversitesi'ndedir. Muhasebe ve bankacılık eğitim müfredatlarında siber güvenlik konusu genellikle farkındalık oluşturacak düzeyde ele alınmıştır.

The threat of cyber attacks on data security has made cyber security important. First of all, associate, bachelor and graduate education programs opened under the name of "cyber security" in 208 universities in Turkey were examined. It has been determined that cyber security training/education is positioned in the field of engineering and natural science. Considering that cyber security is an interdisciplinary subject, the aim of this study is to determine the status of cyber security training in accounting and banking (bachelor) education in the field of social sciences. Content analysis method was used in the study. The curricula of 15 programs in accounting and 43 programs in banking were investigated in terms of cyber security and cyber security-related courses. There are no cyber security and cyber security-related courses in 6 accounting programs and 18 banking programs. Istanbul Aydın University is the only university that offers education under the name of "cyber security" as a course in the curricula of universities that provide accounting education. Erzincan Binali Yıldırım University and Istanbul Nisantasi University offer "cyber security" training as a course in the banking curricula. The richest curricula in terms of cyber security-related courses are at Baskent University among accounting programs and Istanbul Gelisim University among banking programs. In accounting and banking education curricula, cyber security is generally addressed at awareness-raising level.

DOI: <https://doi.org/10.30783/nevsosbilen.1622480>

Atıf/Cite as: Özbıngöl, A. (2025). Türkiye'de "Siber Güvenlik" eğitimine disiplinler arası bakış: Muhasebe ve bankacılık bölümleri açısından bir araştırma. *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi*, 15(2), 777-806.

¹ Bu çalışma, 27-29 Eylül 2024 tarihlerinde "Akıllı Teknolojiler ve Değişen Dünya Dinamikleri" temasıyla Bartın/TÜRKİYE'de düzenlenen "ICAIFR'24, 11. Uluslararası Muhasebe ve Finans Araştırmaları Kongresi"nde sunulan ve "Bildiri Özetleri Kitabı"nda yer alan "Türkiye'de "Siber Güvenlik" Eğitimine Disiplinler Arası Bakış: Muhasebe ve Bankacılık Bölümleri Açısından Bir Araştırma" isimli bildirinin genişletilmesi suretiyle üretilmiştir.

Giriş

Dijitalleşme ile birlikte iş yapma ve iletişim kurma alışkanlıklarımız değişmiştir ve yüz yüze yaptığımız birçok işlem, oluşturulan elektronik altyapı ile dijital ortamlarda yapılabilir hâle gelmiştir. Dolayısıyla insanlar, kurumlar, devletler dijital bir dünya içerisinde farklı dijital araçları kullanarak varlıklarını sürdürmektedir. Yapılan bir araştırmaya göre, dünyada 8.01 milyar insanın 5,44 milyarı cep telefonu kullanıcısı, 5,16 milyarı internet kullanıcısı ve 4,76 milyarı aktif sosyal medya kullanıcısıdır. Türkiye’de ise 85,59 milyon insanın 81,68 milyonu cep telefonu, 71,38 milyonu internet kullanıcısı ve 62,55 milyonu aktif sosyal medya kullanıcısıdır (We Are Social Global ve Türkiye Raporu, 2023). Bu araştırmadaki kullanıcı istatistikleri, dijital ile olan temasımızı net bir şekilde ortaya koymaktadır.

Dijital çağda kullanıcılar siber ekosistemin içerisinde bilinçli veya bilinçsiz bir şekilde hareket etmektedir. Kullanıcıların kullandıkları dijital araçların (bilgisayar, telefon, tablet ve benzeri) her birinde çeşitli veriler depolanmaktadır. Kullanıcı bir şahıs ise kişisel verileri, kurum ise kurumsal verileri, devlet ise kamu/kritik öneme sahip veriler dijital araçlarda muhafaza edilmektedir. Bu çağın en büyük kolaylığı dünyanın herhangi bir yerindeki veriye ne zaman istenirse erişebilme imkânına sahip olmak gibi gözükse de kullanıcının bilinçsizliği, kullanılan sistemlerdeki güvenlik açıkları kötü niyetli kişilerin siber tehdidine maruz kalma riskini doğurur.

Siber tehdit, kötü niyetli kişilerin bir ağ aracılığıyla dijital ortamdaki verilere izinsiz erişmesi ve bu sayede veri ve iletişim sistemlerini devre dışı bırakması ya da çökertmesi şeklinde tanımlanabilir (kku.edu.tr). Siber tehditlerin küresel boyuttaki zararı 2024 yılı için 9,5 trilyon ABD Doları ve 2025 yılı için 10,5 trilyon ABD Doları olarak tahmin edilmiştir (Official Cybercrime Report, 2023). Bu tahmin edilen tutarlar aynı zamanda, tehdidin olduğu bir yerde veri güvenliğinin sağlanabilmesi için katlanılması gereken maliyetin küresel düzeyini de ifade eder. Siber saldırıların tahmini küresel zararının büyüklüğü, bir ülke ekonomisi gibi düşünülürse, ABD ve Çin ekonomilerinden sonra gelen üçüncü büyük ülke ekonomisini temsil edecek boyuttadır (Garanti BBVA, www.garantibbva.com.tr). Bu açıdan siber tehditler karşısında veri güvenliğinin sağlanması ülke ekonomisinin büyümesine katkı sağlarken, aksi durum ülke ekonomisinin küçülmesine neden olacaktır. Bu yüzden veri güvenliğine yönelik siber tehdit, siber güvenliği bireysel, kurumsal, ulusal ve küresel ölçekte çok önemli hâle getirir.

Siber tehdit sistemlerin devre dışı bırakılması suretiyle verilere erişimin engellenmesi, verilerin yok edilmesiyle sınırlı kalmayabilir. 17.09.2024 tarihinde İsrail tarafından Lübnan’a yapılan saldırı (çağrı cihazlarının patlatılması), siber tehdidin “ölüm tehdidi”ni de içerebileceğini ortaya çıkarmıştır. Aynı zamanda bu saldırı eski/yeni fark etmeksizin bir teknolojik ürünün, siber silaha dönüştürülebileceğini göstermiştir. Dolayısıyla siber güvenlik ülkelerin milli güvenliği açısından oldukça önemlidir. Bu noktada da milli teknoloji hamleleri ve yatırımları büyük önem arz etmektedir.

Siber güvenlik, dijital ortamdaki kullanıcı verilerini izinsiz erişimlere karşı korumayı amaçlayan çok boyutlu bir disiplindir. Bu alan; güvenlik politikaları ve prosedürlerinin uygulanmasını, ileri düzey teknolojik çözümlerin kullanılmasını ve kullanıcı farkındalığını artırmaya yönelik eğitim faaliyetlerini içerir. Ayrıca siber güvenlik; hukuki, etik, teknik ve teknolojik boyutların yanı sıra, eğitim, milli güvenlik, savunma stratejileri ve uzay teknolojileri gibi birçok farklı alanla doğrudan ilişkilidir. Siber güvenlik ile kullanıcının (bireylerin, toplumların, özel veya kamu kurum ve kuruluşlarının, devletlerin) bir ağa bağlı dijital ortamdaki verilerinin gizliliği, bütünlüğü ve kullanılabilirliği korunur (Ulah vd., 2019; Aktaran: Admass, Munaye & Diro, 2024: 1). Siber güvenlik kullanıcıların bilgilerinin, varlıklarının, haklarının, mülkiyetlerinin ve mahremiyetlerinin korunmasını sağlar (kku.edu.tr).

Siber tehdit durumu hakkında 2023 yılı Ekim-Aralık dönemi için hazırlanan bir rapora göre, bu dönemde toplam 1.846.547 siber saldırı tespit edilmiş, bunların 227.442’si Rusya, 141.002’si ABD ve 127.283’ü Polonya tarafından gerçekleştirilmiştir (STM, Siber Tehdit Durum Raporu, 2023: 15-16). 2024 yılı Temmuz-Eylül dönemi için hazırlanan raporda ise toplam 1.583.206 siber saldırı tespit edilmiş, bunların 204.709’u Rusya, 126.184’ü Hindistan ve 125.164’ü Çin tarafından gerçekleştirilmiştir (STM, Siber Tehdit Durum Raporu, 2024: 19-20). Farklı dönemlerde hazırlanmış bu iki rapor dünyada en çok siber saldırı yapan ülkenin Rusya olduğunu ortaya çıkarmıştır. Kuzey Amerika, Latin Amerika, Avrupa, Asya Pasifik, Ortadoğu ve Afrika’yı kapsayan siber tehdit savunma raporuna göre son bir yıl (2023) içerisinde 6 veya daha fazla başarılı siber saldırı yaşayan ülkeler sıralamasında Türkiye 11. sırada yer alırken, fidye yazılımı mağdurları sıralamasında Türkiye 10. sırada yer almaktadır. En az bir başarılı siber atak yaşayan sektörler sıralamasına göre, finans sektörü % 95,7 ile 1. ; telekom

ve teknoloji sektörü % 88,9 ile 2.; perakende sektörü % 85,6 ile 3. ; sağlık sektörü % 79,2 ile 4. ; eğitim sektörü %78,9 ile 5.; imalat sektörü % 77,5 ile 6. ve yönetim (hükümetler) % 74,4 ile 7. sırada yer almaktadır (CyberEdge Group, 2023: 8-23). Coğrafi alanı Ortadoğu, Türkiye ve Afrika ile sınırlandıran META (Middle East-Turkey-Africa) iş bölgesinde yapılan bir araştırmaya göre, Türkiye, en çok siber saldırılara maruz kalan ülkeler sıralamasında 1. sırada, en çok fidye ödeyen ülkeler sıralamasında ise 29. sırada yer almıştır. Bu araştırmaya göre Türkiye’yi birinci sırada tutan nedenler arasında coğrafi konumunun önemi, nüfusunun yüksekliği, çevrimiçi tehditlerden en çok etkilenen kullanıcı sayılarının yüksekliği, siber güvenlik farkındalığının azlığı, güvenliğe yeterince bütçe ayrılmayışı gibi nedenler sıralanmıştır (Para Dergisi, 2024). Ulusal Siber Güvenlik Endeksi, küresel ölçekte canlı bir endeks olup ülkelerin siber tehditleri bertaraf edebilme ve siber olayları yönetebilme konusundaki hazırlıklarını ölçmektedir. Bu endeksin ilk üç ülkesi Belçika (94,81), Litvanya (93,51) ve Estonya (93,51) olurken, Türkiye (61,04) endeksin 55. ülkesi olmuştur (NCSE 2016-2023). Gerek ülkemizde gerekse tüm dünyada siber güvenlik dijital çağın en önemli güvenlik meselesidir. Siber ekosistemin içerisinde yer alan her bir bireyin bilinçli ve farkındalığı yüksek olarak hareket edebilmesi için siber güvenlik eğitimi alması oldukça önemli hâle gelmiştir.

Literatür Taraması

Türkiye’de “siber güvenlik ve üniversiteler” konusundaki literatür çalışmaları genel olarak 3 başlık altında incelenebilir:

(I) Türkiye’deki üniversitelerde siber güvenlik eğitime dair yapılan araştırmalar:

Önaçan ve Atan (2016), Türkiye’de siber güvenlik alanında lisans düzeyinde eğitim verilmediğine dikkat çekerken, Deniz Harp Okulu’nun siber güvenlik yüksek lisans programını inceleyerek üniversitelerde siber güvenlik bölümlerinin açılmasının, donanımlı siber güvenlik uzmanlarının yetiştirilmesi ve bu alandaki istihdam ihtiyacının karşılanması açısından büyük önem taşıdığını vurgulamıştır.

Çakır ve Taşer (2023) ise Türkiye siber güvenlik alanındaki kurumlar ve bu kurumların gerçekleştirdiği çalışmaları, yapılan yasal düzenlemeleri, akademik eğitim faaliyetlerini, lisansüstü tezlerde işlenen konuları incelemiştir. Siber güvenlik alanında kamu kurumlarının/kurullarının kurulmasıyla birlikte siber güvenlik alanında kısmi-yetersiz önemlerin yerini ciddi önemlerin aldığı; yapılan yasal düzenlemelere rağmen bilişimle ilgili suçların hukuki yönünde yetersizliklerin olduğu tespit edilmiştir. Ülkemizde 23 üniversitede siber güvenlik bölümünün açıldığı ve siber güvenlik eğitimlerinin verildiği; lisansüstü tezlerde siber güvenlik konusunun siber saldırı, siber savaş, siber suç, siber terör ve siber uzay konularına kıyasla daha çok çalışıldığı belirlenmiştir. Ayrıca, akademik çalışmalardaki artış, yerli ve milli yazılımlardaki yaygınlık ve savunma sanayiinin önder firmalarınca üretilen yazılım-donanım ürünlerinin varlığı ile ülkemizin siber güvenliğinin yakın gelecekte daha iyi düzeylerde olacağı vurgulanmıştır.

(II) Türkiye’de farklı üniversitelerde ve bölümlerde eğitim gören öğrencilerin siber güvenlik farkındalığı ve davranışlarının değerlendirilmesine yönelik çalışmalar:

Karacı, Akyüz ve Bilgici (2017) Kastamonu Üniversitesi’nin “Bilgisayar Mühendisliği” ve “Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE)” ile Ahmet Yesevi Üniversitesi’nin “Bilgisayar Mühendisliği” bölümlerinde eğitim gören öğrencilerin siber güvenlik davranışlarını araştırmıştır. Öğrencilerin güvenlik önlemleri almaları, güvenilmeyen uygulamalardan kaçınmaları, kişisel gizliliklerini koruyabilmeleri, banka-kredi kartı bilgilerini koruyabilmeleri, internet gezintisinden sonra arkalarında iz bırakmayışları şeklindeki davranışların, siber güvenliği sağlamaya yönelik olduğu ve ayrıca internet ve bilgisayar güvenliği konusunda bilgili öğrencilerin siber güvenlik davranışlarının daha olumlu olduğu belirlenmiştir.

Aksoğan, Bayer, Gülada ve Çelik (2018) İnönü Üniversitesi İletişim Fakültesi’nin “Halkla İlişkiler ve Tanıtım” ve “Gazetecilik” bölümü öğrencilerinin siber güvenlik ve siber suçlar farkındalığını araştırmıştır. Siber güvenlik farkındalığı, öğrencilerin genelinde az; erkekler ile interneti daha çok kullananlarda ise daha fazla çıkmıştır. Ayrıca öğrencilerin birçoğu veri hırsızlığının suç olduğunu bilmekle birlikte siber suçu nereye bildireceklerini bilmemektedir.

Eroğlu Yalın ve Şahin Başfıncı (2018) Karadeniz Teknik Üniversitesi İletişim Fakültesi öğrencilerinin siber güvenlik algısını araştırmıştır. Siber güvenlik denilince internet, hacker ve güvenlik kelimelerinin çağrışım yaptığını; siber güvenlik konusunda korku, endişe ve güvensizlik duygularının ön plana çıktığını; öğrencilerin

büyük bir çoğunluğunun siber tehdit ile karşılaşmadığını ancak yakınlarının siber saldırı yaşadığına tanıklık ettiğini ve ayrıca öğrencilerin siber güvenliğin kişisel bilgilerin gizliliği ve güvenliği açısından önemine dair farkındalığının olduğu belirlenmiştir.

Avcı ve Oruç (2020) Türkiye’de bir vakıf üniversitesinin “Eğitim Fakültesi” ile “Mühendislik Fakültesi” öğrencilerinin kişisel siber güvenlik tavırları ile bilgi güvenliği konusundaki farkındalıklarını araştırmıştır. Katılımcıların % 92’sinin kişisel siber güvenlik farkındalığı, bu konularda hiç ders almamalarına rağmen orta; bilgi güvenliği farkındalıkları ise yüksek düzeyde çıkmıştır. Bilgi güvenliği farkındalık düzeyi, mühendislik fakültesi ile sosyal medya hesap sayısı 3’ten çok olanlarda daha yüksek bulunmuştur.

Tokmak (2023) Mehmet Akif Ersoy Üniversitesi’nin “Yönetim Bilişim Sistemleri”, “Muhasebe ve Finansal Yönetim”, “Gümrük İşletme”, “Bilişim Sistemleri ve Teknolojileri” ve “Uluslararası Ticaret” bölümü öğrencilerinin siber güvenlik farkındalığını (gizlilik (I), kontrol/sahiplik (II), bütünlük (III), gerçeklik (IV), erişilebilirlik (V), fayda (VI) faktörleri açısından) makine öğrenmesi yöntemi ile tespit etmek istemiştir. Öğrencilerin siber güvenlik farkındalığının orta düzeyde olduğunu; farkındalığın cinsiyete göre farklılaşmasında sadece bütünlük faktörünün anlamlı fark oluşturduğunu; muhasebe öğrencilerinin farkındalığının az olduğunu; düzeyinin makine öğrenmesi teknikleri ile belirlenebileceğini tespit etmiştir.

Erdal, Filiz ve Budak (2023) Artvin Çoruh Üniversitesi Sağlık Hizmetleri Meslek Yüksekokulu öğrencilerinin kişilik özelliklerinin siber güvenlik algısına etkisini ölçmüştür. Öğrencilerin kişilik özelliklerinden yumuşak başlıklı ön plana çıkarken, nevroitiklik arka planda kalmıştır. Siber güvenlik algısı ölçeğinde güvenilmeyenden kaçışın en yüksek düzeyde, kişisel gizliliği korumanın ise en düşük düzeyde kaldığı saptanmıştır. Kişilik özelliklerinin siber güvenlik algısında önemli etkisinin olmadığı ve farklılıklar oluşturmadığı belirlenmiştir.

Şimşek (2024) bir devlet üniversitesindeki öğrencilerin siber güvenlik farkındalığını, A ve B tipi kişilik tiplerine göre değişkenliğini araştırmıştır. 172 öğrencinin 104’ü A tipi, 68’i ise B tipi kişilik yapısına sahiptir. Öğrencilerin genelinde siber güvenlik farkındalığı “az bilgili” şeklindeyken; A tipi kişiliğe sahip olanlarda siber güvenlik farkındalığının fazla olduğu bulunmuştur.

(III) Türkiye’deki üniversitelerin bilgi işlem daire başkanlıkları ya da akademik personelinin siber güvenlik farkındalığı ve tutumuna ilişkin yapılan araştırmalar:

Tuğal, Almaz ve Sevi (2020) üniversitelerin siber güvenlik sorunlarını tespit etmek ve tespit edilen sorunlara çözüm önerileri sunmak amacıyla araştırma yapmıştır. Siber saldırılar karşısında üniversitelerin teknolojilerinin modernizasyonunun gerekliliği, bilgi sistem altyapılarının güçlendirmesi gerekliliği, bilgi güvenliği için güvenlik politikalarının oluşturulması ve bunlara uyumun sağlanması gerekliliği ve üniversite çalışanlarının ve öğrencilerinin siber farkındalık eğitimi alması gerekliliği sonucuna ulaşılmıştır.

Gündüzalp (2021) Türkiye’deki 206 üniversitenin bilgi işlem daire başkanlıklarında çeşitli pozisyonlarda çalışanların, dijital veri güvenliğini ve siber güvenliği sağlamaya yönelik farkındalıklarını araştırmıştır. Araştırma sonucunda, üniversitelerin bilgi işlem daire başkanlıklarında görev alanların dijital veri güvenliğini ve siber güvenliği sağlama farkındalığının yüksek olduğu; farkındalığın katılımcının yaşına, mesleki deneyimine, eğitim durumuna ve çalıştıkları pozisyonlara göre farklılaştığı belirlenmiştir.

Baz ve Uludağ (2023) ülkemizdeki çeşitli üniversitelerin bilgi işlem daire başkanlıklarında yönetici ve personel pozisyonunda çalışanların siber güvenlik farkındalığının mevcut durumunun tespiti için 23’ü bilgi işlem daire başkanı ve 13’ü mühendis, memur, teknisyen gibi farklı pozisyonlarda görev alan bilgi işlem dairesi çalışanı olmak üzere toplam 36 kişiyle görüşme yapılmıştır. Araştırma sonucuna göre, üniversitelerde öncelikle siber güvenlik farkındalığının oluşturulması gerektiği belirlenmiştir.

Karakaya ve Yetgin (2020) Karabük Üniversitesi’nde görevli akademik ve idari personelin kişisel siber güvenlik algılarını araştırmıştır. Genel itibarıyla çalışanların siber güvenlik farkındalığının olduğunu; akademik/idari konumlarının, yaşlarının ve cinsiyetlerinin kişisel siber güvenlik algısını farklılaştırmadığını; çalışanların siber tehditler için bireysel olarak temel düzeyde bilgisayar güvenliği, şifre güvenliği, internet güvenliği konusunda eğitim desteği alması ve bu bilgileri uygulayabilme yetkinliğine sahip olması gerektiğini saptamıştır.

Araştırma

Araştırmanın Amacı ve Önemi

Siber güvenlik teknik, sosyal ve politik yönleri olması sebebiyle disiplinler arası bir konudur, fen bilimleri ve sosyal bilimleri kapsar. Ülkemizde siber güvenlik ile üniversiteleri ele alan çalışmalarda, siber güvenlik eğitiminden daha çok öğrencilerin, akademik/idari personelin siber güvenlik farkındalığı araştırılmıştır. Siber güvenlik eğitimi kapsamında Çakır ve Taşer (2023) ülkemizde siber güvenlik bölümü olan üniversiteleri sıralarken, Önaçan ve Atan (2016) Deniz Harp Okulu'ndaki siber güvenlik yüksek lisans programını incelemiştir.

Siber güvenliğin disiplinler arası bir konu olmasından hareket edilerek, bu çalışmanın amacı, sosyal bilimler alanında muhasebe ve bankacılık (lisans) eğitiminde siber güvenlik eğitiminin durumunu belirlemektir. Muhasebe ve bankacılık bölümlerinde siber güvenlik hayati bir öneme sahiptir. Çünkü muhasebe ve bankacılık alanında yüksek hacimli finansal veriler işlenmektedir. Kötü niyetli kişiler, bu verilere fidye yazılımları ile erişim imkânının sınırlandırmakta, bu verilerin yer aldığı sistemleri çöktürmekte, çeşitli yöntemlerle siber dolandırıcılık faaliyetleri gerçekleştirmektedir. Dolayısıyla muhasebe ve bankacılık mesleği siber tehditlere açıktır ve bunlara karşı hassasiyet göstermektedir. Muhasebe ve bankacılık eğitimi teknolojik (bilgisayarlı muhasebe, dijital dönüşüm, dijital okuryazarlık, yapay zekâ, blokzincir, nesnelerin interneti gibi dersler ile) eğitimle desteklendiği gibi teknolojik alanda güvenliğin sağlanması açısından siber güvenlik eğitimi ile desteklenmelidir. Bu düşünceden hareketle, muhasebe ve bankacılık müfredatının incelenmesi ihtiyacı doğmuştur. Siber güvenlik literatürü incelendiğinde, ülkemizde siber güvenliğe yönelik farkındalığın ölçülmesine yönelik yapılan araştırmalara rastlanırken, siber güvenlik müfredatının araştırılmasına yönelik herhangi bir çalışmaya rastlanmamıştır. Araştırma, siber güvenlik müfredatlarını ele alması ve siber güvenlik müfredatlarına yönelik disiplinler arası bir karşılaştırma içermesi açısından özgün nitelikte olup, literatüre önemli katkı sağlayacaktır.

Araştırmanın Kapsamı ve Yöntemi

Araştırma üç bölümden oluşmaktadır. Birinci bölümde Türkiye'deki üniversiteleri siber güvenlik yetkinlikleri ve siber güvenlik faaliyetleri; ikinci bölümde “siber güvenlik” adı altında açılan programlar ve müfredatları; üçüncü bölümde ise siber güvenliğin muhasebe ile bankacılık bölümleri açısından sosyal bilimlerdeki iz düşümü araştırılmıştır.

Araştırma kapsamında aşağıdaki sorulara cevap aranmıştır:

- (1) Ülkemizdeki üniversiteler kendilerini “siber saldırılara karşı koruyabilme” yetkinliğine sahip midir?
- (2) Üniversitelerde “siber güvenlik” adı altında yapılan faaliyetler nelerdir?
- (3) “Siber güvenlik” adı altında açılan programlar hangi üniversitelerde yer almaktadır ve hangi düzeyde (ön lisans, lisans, yüksek lisans, doktora) eğitim imkânı sunmaktadır?
- (4) “Siber güvenlik” adı altında açılan programların ders müfredatında hangi dersler yer almaktadır?
- (5) Sosyal bilimler – “Muhasebe ve Finans Yönetimi” bölümlerinde “siber güvenlik”in ele alınış biçimi yeterli midir?
- (6) Sosyal bilimler – “Bankacılık”, “Bankacılık ve Finans”, “Bankacılık ve Sigortacılık”, “Finans ve Bankacılık” programlarında “siber güvenlik”in ele alınış biçimi yeterli midir?

Araştırmada içerik analizi yöntemi kullanılmıştır. İçerik analizinin yapılabilmesi için Türkiye'deki 208 üniversitenin internet sitesi 01.08.2024-25.09.2024 tarihleri arasında taranmıştır.

Birinci araştırma sorusu kapsamında, üniversitelerin kendilerini siber saldırılara karşı koruyabilme yetkinliklerini temsil eden ISO 27001 Sertifikasına sahiplik durumunun belirlenebilmesi için, Türkiye'deki 208 üniversitenin internet sitesinde site içi arama yapılmıştır. Bazı üniversitelerin bu sertifikalarını yayınlamış olduğu, bazılarının ise bu sertifikaya sahip olduğu bilgisini paylaştığı tespit edilmiştir. Sertifika kapsamındaki veriler, Microsoft Excel programında,

- üniversitelerin sertifikaya sahip olup olmadığı,
- sertifikanın türü,
- son geçerlilik tarihi,
- sertifikanın görüntüsünün/sertifika sahiplik bilgisinin yayınlanıp yayınlanmadığı

açısından işlenmiştir.

İkinci araştırma sorusu kapsamında, üniversitelerin siber güvenlik adıyla gerçekleştirdikleri faaliyetlerin tespiti için Türkiye’deki 208 üniversitenin web sitesinde yer alan “duyurular”, “haberler”, “etkinlikler” gibi başlıklar (01.08.2024-25.09.2024 tarihleri arasında) güncel ve geçmişe yönelik olarak taranmış ve siber güvenlik ile ilgili veriler toplanmıştır. Toplanan veriler detaylı bir biçimde okunmuş, araştırma sorusu kapsamında, araştırılan konuya ilişkin olarak öne çıkan hususlar,

- siber güvenlik tanıtım ve farkındalık faaliyetleri,
- siber güvenlik ve kariyer fırsatları,
- siber güvenlik burs ve iş imkânları,
- sertifikalı programlar,
- uygulamalı eğitimler,
- yarışmalar,
- kamplar, yaz okulları, kış okulları,
- siber güvenlik ve hukuk,
- siber vatan,
- siber güvenlik ve yönetim bilişim sistemleri,
- atölyeler,
- festivaller,
- zirveler/kongreler,
- çalıştaylar,
- raporlar,
- işletme ziyaretleri/teknik geziler,
- ortaklıklar/iş birliği anlaşmaları,
- projeler,
- merkezler,
- liselere/12. sınıflara/mezunlara yönelik etkinlikler,
- toplumun farklı kesimlerine yönelik siber güvenlik eğitimi

gibi başlıklar altında kategorize edilmiştir.

Üçüncü araştırma sorusu kapsamında, “Siber güvenlik” adıyla açılan eğitim programları Yükseköğretim Kurulu (YÖK)’nun internet sitesindeki araçlar (ön lisans, lisans atlası gibi) kullanılarak belirlenmiştir. Lisansüstü eğitimler içinse bütün üniversitelerin “enstitü” sayfaları taranmıştır. İlgili araçlar kullanılarak Türkiye’de “Siber güvenlik” adıyla açılan bölümler sayısal olarak tespit edilmiş ve bunların genellikle fen bilimleri alanında konumlandırıldığı belirlenmiştir.

Dördüncü araştırma sorusu kapsamında, fen bilimleri alanındaki siber güvenlik ders müfredatları, üniversitelerin web sitelerinden/Bologna sisteminden çekilmiştir. Ders müfredatlarında yer alan dersler isim ve içerik açısından detaylı bir biçimde okunmuştur. 600’ü aşkın ders isim ve konu benzerlikleri açısından Microsoft Excel programında sınıflandırılmıştır. Fen bilimleri alanında konumlandırılan siber güvenlik programlarında toplam 24 ana ders kategorisi elde edilmiştir. 24 ana ders kategorisi, “siber güvenlik” adı altında açılan programlarda yer alan derslerin, genel görüntüsünü (büyük resmini) vermesi açısından önemlidir. Büyük resme bakıldığında, siber güvenlik programlarındaki müfredatlar, siber güvenliğin teknik yönü, dijital dönüşüm yönü ve hukuki yönü dikkate alınarak oluşturulmuştur. Ayrıca her bir ana kategorinin altında o kategoriye giren dersler belirlenmiştir. Konu bütünlüğünün sağlanması (korunması) açısından sadece siber güvenlik ana kategorisine giren 70 dersin ismi verilmiştir.

Beşinci ve altıncı araştırma sorusu kapsamında, siber güvenlik eğitiminin fen bilimlerindeki ve sosyal bilimlerdeki durumunun tespiti ile disiplinler arası ilişkinin kurulması düşünülmüştür. Siber güvenlik eğitiminin sosyal bilimlerdeki iz düşümünün belirlenebilmesi için fen bilimleri alanında verilen dersler ile sosyal bilimlerdeki belirtilen bölümlerdeki ders müfredatlarının durumu araştırılmıştır. Öncelikle YÖK Lisans Atlası’ndan faydalanılarak Muhasebe ve Finans Yönetimi bölümü ile bankacılık bölümü olan üniversiteler belirlenmiştir. Belirlenen üniversitelerin internet sitelerinden/Bologna sisteminden ders kataloglarına ulaşılmıştır. Ders kataloglarındaki dersler isim ve içerik açısından incelenmiştir. Ardından fen bilimlerindeki siber güvenlik müfredatları ile sosyal bilimlerdeki siber güvenlik müfredatları karşılaştırılarak yeterlilik durumu tartışılmıştır.

Araştırmanın Bulguları

Dijital çağın en önemli konusu siber güveniktir ve tüm toplumda siber güvenlik farkındalığının oluşturulmasının yolu ise eğitimden geçmektedir. Dijital ile olan temas, üniversitelere bilinçli ve donanımlı iş gücü yetiştirme görevi yüklemektedir. Araştırma kapsamında elde edilen bulgular aşağıda sıralanmıştır:

- 208 üniversiteden 61’i ISO 27001 sertifikasına sahipken, sadece 5’i ISO 27001:2022 sertifikasına sahiptir. 2 üniversite ise bu sertifikaya geçiş aşamasındadır.

- 11 üniversitenin “ücretli sponsorlu reklam” adı altında sahte web sitelerinin yapıldığı belirlenmiştir. Ayrıca 11 üniversitenin 4’ü ISO 27001 sertifikasına da sahiptir.
- Türkiye’de sadece 4 üniversite, internet sitesinde, akademik/idari personel ile öğrencileri uyaran, siber güvenlik farkındalığını artıran/uyarıcı metin yayınlamıştır. Ancak bu metinlerde siber saldırıya maruz kalınması halinde başvurulacak yerler konusunda sadece bir üniversite bilinçlendirme yapmıştır.
- Türkiye’deki 208 üniversitenin 124’ünde; 81 ilin 63’ünde siber güvenlik faaliyetleri gerçekleştirilmiştir. En çok yapılan ilk üç faaliyetin konusu, “siber güvenlik tanıtım ve farkındalık faaliyeti”, “siber güvenlik ve kariyer fırsatları” ile “siber vatan”dır.
- 208 üniversitenin 22’sinde siber güvenlik adı altında bir program açılmıştır. Programların 5’i ön lisans, 1’i lisans, 19’u yüksek lisans ve 2’si doktora düzeyindedir.
- Siber güvenlik programları çoğunlukla fen bilimleri alanında konumlandırılmıştır. Siber güvenlik ders müfredatları sadece teknik altyapı boyutuyla tasarlanmamış, aynı zamanda siber güvenliğin sınırlar ötesi boyutu (siber savaş) ve etik - siber hukuk boyutu düşünülerek hazırlanmıştır. Ayrıca ders müfredatlarında dijital dönüşüm ile siber güvenlik arasındaki bağ kurulmuştur. Yani müfredatlar da bulut bilişim dersi yer aldığı gibi bulut bilişimde siber güvenlik dersi de yer almıştır. Müfredatlarda etik ve siber hukuk dersleri vardır ve dönemlik olarak açılmaktadır. Siber hukuk dersleri ulusal ve uluslararası düzenlemeleri kapsayacak şekilde zengin bir içerikle oluşturulmuştur.
- Sosyal bilimler, muhasebe ve finans yönetimi bölümlerinde seçmeli dahi olsa “siber güvenlik” adında bir ders sadece İstanbul Aydın Üniversitesi’nin ders kataloğunda vardır. Muhasebe programlarında siber güvenlik ile ilişkili dersler açısından en çok ders Başkent Üniversitesi’nin müfredatında vardır. Bu programlarda “siber hukuk” adıyla ayrı bir dersin açılmadığı, siber hukukla ilişki olan derslerde ise siber hukukun üstünkörü ele alındığı belirlenmiştir.
- Sosyal bilimler, bankacılık bölümlerinde seçmeli dahi olsa “siber güvenlik” isimli ayrı bir ders Erzincan Binali Yıldırım Üniversitesi ile İstanbul Nişantaşı Üniversitesi’nde vardır. Programlar arasında siber güvenlik ile ilişkili dersler açısından en çok ders İstanbul Gelişim Üniversitesi’nin müfredatında vardır. Bankacılık programlarında “siber hukuk” adıyla ayrı bir ders açılmadığı, siber hukukla ilişki olan derslerde ise siber hukukun yüzeysel ele alındığı belirlenmiştir.

Araştırmanın Kısıtları

Bu araştırmanın kısıtları şöyledir:

- Araştırmada üniversitelerin ön lisans, lisans ve lisansüstü eğitim programları için, program isminde “siber güvenlik” ifadesi geçenler esas alınmıştır. Dolayısıyla siber güvenlikle ilişkili olabilecek veri bilimi ve analitiği, bilgi güvenliği teknolojisi, bilişim sistemleri ve teknolojileri, yönetim bilişim sistemleri gibi bölümler kapsam dışı bırakılmıştır.
- Sabancı Üniversitesi’nin doktora, Yıldız Teknik Üniversitesi’nin yüksek lisans ders müfredatına ulaşamamıştır.
- Türkiye’de “Bankacılık”, “Bankacılık ve Finans”, “Bankacılık ve Sigortacılık” ve “Finans ve Bankacılık” adı altındaki programlar incelenmiştir. Dolayısıyla başka isimlerle açılanlar (uluslararası bankacılık vb².) kapsam dışı bırakılmıştır.
- Belirtilen kriterde bankacılık bölümü olan İstanbul Medipol Üniversitesi ile Munzur Üniversitesi’nin müfredat bilgisine ulaşamamıştır.

Türkiye’deki Üniversitelerin Siber Güvenlik Yetkinlikleri ve Siber Güvenlik Faaliyetleri

Türkiye’deki Üniversitelerin Siber Güvenlik Yetkinlikleri ve Üniversitelerin Kurumsal Kimliğini Hedef Alan Siber Tehditlerin Varlığı

Bir ülkenin eğitim sisteminde en üst düzey eğitimi veren kuruluşlar üniversitelerdir ve dijital çağda siber güvenlik konusunda iş gücünün yetiştirilmesi açısından lokomotif görevi üstlenmelidir (Baz & Uludağ, 2023: 412). Üniversiteler günümüz koşullarında öğrencilerine akıllı cihazlardan ulaşabilecekleri uygulamalar için ve uzaktan

² vb: “ve benzeri” ifadesinin kısaltmasıdır.

eğitim verebilmek için bilişim ve teknoloji yatırımları yapmaktadır. Üniversiteler pek çok veriyi (istihdam sağladığı akademik/idari personel verilerini, eğitim verdiği öğrencilerin verilerini, tüm eğitim birimlerinin verilerini, idari birimlerinin verilerini, varsa üniversiteye ait kuruluşların verilerini) dijital ortamda muhafaza etmektedir. Ayrıca üniversiteler, internet sitelerinde kuruma ilişkin duyuru, ilan, etkinlik gibi güncel haberleri ve bunların arşivlerini de kullanıcıların istifadesine sunmaktadır. Üniversiteler sosyal medya hesapları aracılığıyla da anlık bilgi paylaşımında bulunmaktadır.

Eğitim kurumlarının bu kadar yüklü ve çeşitli veriyi barındırması, siber saldırıda bulunanları cezbetmiştir. En az bir başarılı atak yaşayan sektör sıralamasında eğitim sektörü % 78,9 ile 5. sıradadır. Üniversiteler dijital ortamdaki verilerinin bütünlüğü, gizliliği ve kullanılabilirliğini siber saldırılara karşı korumak için siber güvenlik önlemleri almalıdır. Üniversiteler kendilerini hedef alan siber tehditler karşısında proaktif bir yaklaşım sergileyerek kendi bünyelerinde ayrı bir merkez açabilir (Örneğin Kayseri Üniversitesi -“Siber Güvenlik Uygulama ve Araştırma Merkezleri”), mevcut yapılarını güçlendirebilir ve kullanıcılarını (akademik/idari personel, öğrenci, ücretli/sertifikalı hizmetlerden faydalanan isteyen diğer kişileri, araştırmacıları) bilgilendirebilir.

Şüphesiz üniversiteler kendilerini siber saldırılardan korumak için bilgi işlem daire başkanlıkları aracılığıyla gerekli tedbirleri almıştır. Ancak bazı üniversiteler kendi verilerini siber saldırılara karşı koruyabilme yetkinliğini bir üst noktaya taşımış, ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) sertifikası alarak bu yetkinliklerini taçlandırmıştır. ISO 27001 BGYS, kurumsal bilgi güvenliğinin sağlanabilmesi için insanları, süreçleri ve bilgi sistemlerini kapsayan ve üst yönetimce desteklenen bir yönetim sistemidir (<https://belgelendirme.ctr.com.tr/iso-27001.html>). Bu sertifika tüm dünyada geçerliliği olan; bir kuruluşun bilgi güvenliği konusundaki yetkinliğini uluslararası düzeyde tescilleyen; verilerin bütünlüğünü, gizliliğini ve bilgiye erişilebilirliğe ilişkin güvenlik ihlallerinin en aza indirildiğini gösteren bir belgedir (www.bilgi.edu.tr) ve aynı zamanda bir kuruluşun bilgi güvenlik yönetim sisteminin belirli standartlarda olduğunu göstermektedir. Geçerlilik süresi 3 yıl olan bu sertifikanın ISO 27001:2005, ISO 27001:2013, ISO 27001:2017 ve ISO 27001:2022 gibi çeşitleri bulunmaktadır. ISO 27001:2022 sertifikası bir kuruluşun BGYS’nin siber saldırılara karşı da yetkinliğini gösterir (www.iso.org).

Ülkemizdeki 208 üniversitenin internet siteleri ISO 27001 BGYS sertifikasına sahip olup olmadıkları açısından taranmıştır. 208 üniversitenin 61’i yani (61/208=) % 29’u ISO 27001 BGYS sertifikasına sahip iken, % 71’i ISO 27001 BGYS sertifikasına sahip değildir. 61 üniversitenin 36’sı ISO 27001 sertifikalarını kendi internet sitesinde yayınlarken, 25’i ise sertifikasının var olduğu bilgisini duyurmuştur. Sertifikasını yayınlayan 36 üniversitenin 22’sinde sertifikanın geçerlilik süresinin dolduğu tespit edilmiştir. Sertifika geçerlilik süresi dolan üniversitelerin bilgi güvenliği yönetim sistemlerindeki yetkinlik süreçlerini yeniden gözden geçirip, varsa eksikliklerini tamamlayarak ISO’ya başvurmaları gerektiği düşünülmektedir. Ülkemizdeki 208 üniversiteden sadece 5’i (Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi, Ankara Hacı Bayram Veli Üniversitesi, Fırat Üniversitesi, Kastamonu Üniversitesi, Sağlık Bilimleri Üniversitesi) BGYS’nin siber saldırılara karşıda yetkin olduğunu gösteren ISO 27001:2022 sertifikasına sahiptir. Ted Üniversitesi ile Kırşehir Ahi Evran Üniversitesi ise bu sertifikaya geçiş aşamasındadır.

Bilinçli internet kullanıcıları özellikle bankaların ya da alışveriş sitelerinin “ücretli sponsorlu reklam” adı altında sahte web sitelerinin olduğunu bilirler. Kötü niyetli kişiler sahte siteler aracılığıyla kullanıcı bilgilerini ele geçirmekte ve onları maddi ve manevi zarara uğratmaktadır. Araştırma sırasında Türkiye’deki üniversitelerden 1’i devlet üniversitesi (Kafkas Üniversitesi) ve 10’u vakıf üniversitesi (Altınbaş Üniversitesi, İstanbul Beykent Üniversitesi, İstanbul Galata Üniversitesi, İstanbul Gedik Üniversitesi, İstanbul Gelişim Üniversitesi, İstanbul Kent Üniversitesi, KTO Karatay Üniversitesi, Kapadokya Üniversitesi, Kavram Meslek Yüksekokulu, Şişli Meslek Yüksekokulu) olmak üzere toplam 11 üniversitenin “ücretli sponsorlu reklam” adıyla sahte sitelerinin yapıldığı belirlenmiştir.³ Bu durum, kötü niyetli kişilerin bankalar ve alışveriş sitelerinden sonra vakıf üniversitelerini hedef aldığını gösterir. Ayrıca ISO 27001 BGYS sertifikasına sahip üniversitelerin sahte sitelerinin yapılmış olması ihtimalinden yola çıkarak araştırma yapıldığında ise İstanbul Beykent Üniversitesi, İstanbul Gedik Üniversitesi, İstanbul Gelişim Üniversitesi, KTO Karatay Üniversitesi’nin bu durumda olduğu belirlenmiştir.

³ Çalışma sırasında ücretli sponsorlu reklam adı altında açılan sahte web sitelerinin günün farklı saatlerinde ortaya çıktığı tespit edilmiştir.

Tespit edilen bu bulgular bilgi güvenliğinin, sadece teknolojik önlemler alınarak ya da kurum/kuruluşların bilgi güvenliği yönetim sistemlerinin ISO'larla taçlandırılması suretiyle sağlanamayacağını göstermiştir. “Bir zincir ancak en zayıf halkası kadar kuvvetlidir” (www.gelisim.edu.tr) prensibiyle kullanıcıların eğitilmesi ve farkındalığının artırılması gerekir. 208 üniversitenin sadece 4’ü internet sitesinde, kullanıcıları uyaran bir bilgi paylaşımı yapmıştır. Afyon Kocatepe Üniversitesi “*Siber Güvenlik Uyarısı*”, Necmettin Erbakan Üniversitesi “*Dikkat Tuzak Var - Siber Farkındalık Çalışmaları*”, Ordu Üniversitesi “*Siber Güvenlik Duyurusu*”, Kırıkkale Üniversitesi “*Kurumsal Siber Güvenlik Önlemleri Bağlamında Kurumsal E-Postalarda Dikkat Edilmesi Gereken Hususlar*” başlığı altında siber güvenlik farkındalığını artırıcı/uyarıcı metin yayınlamıştır. Bu metinlerde özellikle eski sürüm işletim sistemlerinin güncellenmesi, anti virüs programlarının kontrollerinin yapılması, e-postalar için güçlü parola oluşturulması, bilinmeyen adreslerden gelen e-postaların açılmaması, “kurumdan uzaklaştırılanlar listesi” ya da “izinlerin iptali” ifadelerini içeren e-postaların birer fidye yazılım olabileceği hususu, ücretsiz wifi ve mobil uygulama riskleri vurgulanmıştır. Bir siber saldırıyla karşılaşılması halinde, nereye/nasıl başvuru yapılabileceği konusunda bir bilgiye sadece Afyon Kocatepe Üniversitesi yer vermiştir. Üniversiteler kendi kurumsal kimliğine yöneltile siber tehditler/teknolojik suistimaller karşısında kullanıcılarını uyarıcı ve aydınlatıcı bildirimler yaparak bilinçlendirmelidir. Ayrıca siber saldırıya maruz kalınması halinde başvurulacak makamları da belirtmelidir. Dört üniversitenin yayınladığı siber güvenlik farkındalık metinlerinde dikkat çekilen hususlara ilave olarak, örneğin “ücretli sponsorlu reklam” sayfası adı altında taklit edilen bir siteden giriş yapmadığınıza emin olunuz. Kişisel/banka bilgilerinizi paylaşmayınız. Şüpheli durumda ... birim/... numara ile 7/24 iletişime geçiniz şeklindeki bildirimlerin pop-up (otomatik açılır pencere)⁴ olarak üniversitelerin internet sitesinde verilmesinin uygun olacağı düşünülmektedir.

Türkiye’deki Üniversitelerde Siber Güvenlik Kapsamında Gerçekleştirilen Faaliyetler

Türkiye’deki 208 üniversitenin internet sitesindeki duyurular, haberler, etkinlikler sayfası taranmış ve siber güvenlik kapsamındaki paylaşımları incelenmiştir. 208 üniversitenin 124’ünde (% 59,61’inde) ve 81 ilin 63’ünde (% 77,77’sinde) siber güvenlik konulu faaliyetlerin gerçekleştirildiği tespit edilmiştir. Üniversitelerimizde, ülkemizin doğusundan batısına, kuzeyinden güneyine siber güvenlik konusunda muazzam bir çabanın verildiği görülmüştür.

Siber güvenlik adı altında gerçekleştirilen faaliyetler, üniversitelerin web sitelerinden toplanmış, detaylı bir biçimde incelenmiş, gerçekleştirilen yüzlerce faaliyete dair dağınık ve farklı türdeki bilgilerin derli toplu bir biçimde sunumunun yapılabilmesi için, öne çıkan hususlar bir araya getirilmiş ve sınıflandırma yapılmıştır. Bu sınıflandırma aslında zihin tarafından yapılan, kendiliğinden oluşan doğal bir sınıflandırmadır⁵ ve Eleanor Rosch’un Prototip Teorisi ile örtüşmektedir. Rosch’un “Doğal Kategoriler” (Natural Categories)” çalışmasına göre prototip, belirgin bir konuma sahip uyarıcıdır ve bir kategorinin oluşumunda o kategoriyle ilişkilendirilebilecek ilk uyarıcıdır şeklinde tanımlanmıştır (https://tr.wikipedia.org/). Prototip, insan zihnindeki bir kavramın en temsil edici (en tipik) örneği olduğundan, insanlar kavramları kategorize ederken prototiplere güvenirlir (https://helpfulprofessor.com/). Buna göre, üniversitelerin yaygın olarak gerçekleştirdiği siber güvenlik faaliyetleri, benzerlikleri (öne çıkan yönleri) açısından sınıflandırıldığından ve bu sınıflandırmalar belirli tipik örnekler⁶ etrafında şekillendirildiğinden Prototip Teorisi’ne uygundur. Üniversitelerin siber güvenlik kapsamında gerçekleştirdiği faaliyetler kategorize edilerek Tablo 1.’de sunulmuştur.

Tablo 1. Türkiye'deki Üniversitelerin Siber Güvenlik Faaliyetleri

Kategori Adı	Siber Güvenlik Faaliyetlerinin Türleri	Siber Güvenlik Faaliyetinin Gerçekleştirildiği Üniversitelerin Adı
Üniversite ile Güvenlik Güçleri	Siber Güvenlik, Çevirim İçi Güvenlik, Dijital Farkındalık, Siber Suçlar, Siber	Aksaray, Anadolu, Ardahan, Artvin Çoruh, Aydın Adnan Menderes, Bandırma Onyedi Eylül, Bartın,

⁴ İnternet kullanıcılarının bir web sitesini ziyaret ettiğinde/her ziyaret edişinde açılan küçük bilgilendirme penceredir ve kullanıcıyı bilgilendirmek, kullanıcıyı bir fiile yönlendirmek veya kurum/ürün reklamını yapmak amacıyla kullanılmaktadır (www.userspots.com).

⁵ Bu açıklamalar hangi teori kapsamında değerlendirilmelidir? diye ChatGPT’ye sorulduğunda, *bu açıklamalar “zihin tarafından yapılan doğal sınıflandırma” vurgusu nedeniyle Gestalt Teorisi veya Prototip Teorisi kapsamında değerlendirilebilir* şeklinde cevap alınmıştır.

⁶ Örneğin siber güvenlik tanıtım ve farkındalık faaliyeti gibi bir prototip (tipik örnek) zihinde şekillendiğinde, zihin o kapsamda yapılan eylemleri bir araya getirme faaliyetini gerçekleştirmektedir.

(İl Emniyet Müdürlüğü, İl Jandarma Komutanlığı) İşbirliğiyle Gerçekleştirilen; Teknoloji Transfer Ofisleri, Öğrenci Toplulukları, Bilgi İşlem Daire Başkanlıkları vb. Tarafından Gerçekleştirilen Tanıtım ve Farkındalık Faaliyetleri	Zorbalık, Dijital Zorbalık, Fidyе Yazılımı, Dijital Yılmazlık (Dayanıklılık), Hacker'lık, Siber Zorbalıktan Korunma Yolları, Siber Olaylarla Mücadele, Siber Tehditler, Siber ve Narkotik Suçlarla Mücadele Konularında Bilgilendirme	Bayburt, Biruni, Çankaya, Çankırı Karatekin, Erciyes, Erzurum Teknik, Fatih Sultan Mehmet Vakıf, Fırat, Gazi, Gaziantep İslam Bilim ve Teknoloji, Gümüşhane, Iğdır, İnönü, İstanbul Aydın, İstanbul Kültür, İstanbul Medeniyet, İstanbul Ticaret, İstinye, İzmir Katip Çelebi, Karamanoğlu Mehmetbey, Kırıkkale, Kilis 7 Aralık, Konya Teknik, Muğla Sıtkı Koçman, Munzur, Necmettin Erbakan, Nevşehir Hacı Bektaş Veli, Niğde Ömer Halisdemir, Ondokuz Mayıs, Marmara, Orta Doğu Teknik, Ostim Teknik, Sağlık Bilimleri, Sakarya, Samsun, Selçuk, Sinop, Sivas Bilim ve Teknoloji, Tekirdağ Namık Kemal, Trabzon, TOBB Ekonomi ve Teknoloji, Üsküdar, Yalova, Yüksek İhtisas, Zonguldak Bülent Ecevit
Siber Güvenlik ve Kariyer Fırsatları	Dijital Dünyada Girişimcilik, Siber Güvenlik Girişimcilerine İlişkin Eğitim/Mentorluk Programı, Siber Güvenlikte Kariyer Fırsatlarına İlişkin Mezunlar, Siber Güvenlik Uzmanları, Teknoloji Liderleri, Sektörün Öncü Firmaları ile Yapılan Söyleşiler /Etkinlikler	Afyon Kocatepe, Ataşehir Adı Güzel Meslek Yüksekokulu, Bandırma Onyedi Eylül, Beykoz, Bilkent, Eskişehir Teknik, Fatih Sultan Mehmet Vakıf, Fırat, Haliç, Hasan Kalyoncu, İstanbul/Cerrahpaşa, İstanbul Bilgi, İstanbul Kent, İstanbul Kültür, İstanbul Nişantaşı, İstanbul Sabahattin Zaim, İstanbul Teknik, İstanbul Topkapı, İstinye, Karadeniz Teknik, Kastamonu, Kırıkkale, Muş Alparslan, Recep Tayyip Erdoğan, Sakarya, Ted, Yeditepe, Tekirdağ Namık Kemal, Yozgat Bozok
Siber Güvenlik Burs ve İş İmkânları	Eğitim Bursu/Barikat İnternet Güvenliği Bilişim A.Ş.	Fırat
	Karşılıksız Burs/CCNA CYBEROPS Firması	Gaziantep
	Akademik Yapay Zekâ ve Robotik Bursu	Haliç
	İstihdam İmkânı/Siber Akademi Projesi'ni Başarıyla Bitiren İlk 60 Kişi	İstanbul Gelişim
	İş Garantili/ Siber Güvenlik Eğitimi	İstanbul Aydın
Sertifikalı Programlar	Siber Güvenlik Eğitimi	İstanbul Aydın, İstanbul Sabahattin Zaim, Manisa Celal Bayar Üniversitesi ile Kalkınma Ajansları Genel Müdürlüğü İşbirliği.
	Siber Güvenlik Eğitimi/HPC Sertifikalı	Harran
	İş Garantili Siber Güvenlik Eğitimi	İstanbul Aydın
	Siber Güvenlik ve Ağ Yönetimi	Artvin Çoruh, Hitit, Kilis 7 Aralık
	Siber Güvenlik Uzmanlığı/Teknisyenliği Eğitimi	Başkent, Kocaeli Sağlık ve Teknoloji Üniversitesi ile EC-Council İşbirliği, KTO Karatay
	Siber Güvenlik ve Siber Olaylara Müdahale Eğitimi	İstanbul Aydın
	Beyaz Şapkalı Hacker Eğitimi	Başkent
	Siber Analist SOC Eğitimi	Başkent
Uygulamalı Eğitimler	Siber Güvenlik Temel Seviye	Hakkari
	Siber Güvenlik ve SOC Analist Eğitimi	İstanbul Gedik
	Siber Güvenlik ve Ağ Yönetimi	Bingöl
	Siber Güvenlik	Çanakkale Onsekiz Mart Üniversitesi ile Google Developer Students Clup İşbirliği, Giresun, Mersin, Ted
	Siber Güvenlik ve Bilgi Güvenliği	Bartın
	Uçtan Uca Siber Güvenlik	Ankara Hacı Bayram Veli
	Siber Güvenlikte Kullanılan Ürünler	Fırat

	Siber Güvenlik ve React Native	Fırat
	Beyaz Şapkalı Hacker	Kastamonu, Kırıkkale, Kocaeli Sağlık ve Teknoloji
	Siber Güvenlik ve Sızma Testi Farkındalık	İstanbul Topkapı
	Sızma, Sızma Testi ve Siber Güvenlikte Defans	Beykoz, İstanbul Medeniyet Üniversitesi ile STM İşbirliği, Kahramanmaraş Sütçü İmam, Sinop
	Siber Güvenlik ve Yazılım	Burdur Mehmet Akif Ersoy
	Zararlı Yazılım Analizi, Linux Kampı, Geleneksel Siber Güvenlik Eğitimi	Karadeniz Teknik
	Siber Güvenlik Fikir Yarışması	Ardahan, İstanbul Ticaret
	Hayal Edin Gerçekleştirilim Sosyal İnovasyon Fikir Yarışması	İstanbul Kültür
	Siber Güvenlik Bitirme Projeleri Yarışması	Artvin Çoruh, Gaziantep İslam Bilim ve Teknoloji, İstanbul Gedik
	“Capture the Flag” Bayrağı Yakala Yarışması	Bahçeşehir, Fırat, Karadeniz Teknik
Yarışmalar	Üniversiteler Arası Siber Savunma Yarışması	Ardahan, Marmara
	Hackathon	Hasan Kalyoncu, İstanbul Aydın, Kahramanmaraş Sütçü İmam, Manisa Celal Bayar, Samsun, Toros
	Siber Güvenlik Uzmanlığı Yarışması/Öğrenci Başarısı Paylaşımı	Ostim Teknik
	Teknopark İstanbul Siber Güvenlik Yarışması/Öğrenci Başarısı Paylaşımı	Özyeğin
Kamplar, Yaz Okulları, Kış Okulları	Siber Güvenlik Kampı	Ankara, Ardahan, Aydın Adnan Menderes, Düzce, Fatih Sultan Mehmet Vakıf, Fırat, Gazi, Kırıkkale
	Siber Güvenlik ve Java Kampı	Zonguldak Bülent Ecevit (Gençlik ve Spor Bakanlığı, Zonguldak Belediyesi, BTK Akademi ve USOM İşbirliği)
	Siber Güvenlik Kış Kampı	Bahçeşehir, Ted
	12. Sınıf ile Mezunları Kapsayan Siber Güvenlik Kampı/Liselere Yönelik Siber Güvenlik Yaz Kampı	Kadir Has
	Cyber MACS Programı İlk Yaz ve İlk Kış Okulu	Kadir Has
Siber Güvenlik ve Hukuk	Kişisel Verilerin Korunması Kanunu, Bilgi Güvenliği, Gizlilik, Siber Güvenlik Konularında Farkındalık Eğitimleri	Altınbaş, Bahçeşehir, Bandırma Onyediy Eylül, Çankaya, Galatasaray, Konya Gıda ve Tarım, Marmara, Muğla Sıtkı Koçman
	Bilişim Suçları, Bilişim Hukuku, Adli Bilişim, Adli Bilişim ve Siber Güvenlik Uygulamaları, Mukayeseli Hukuk ve İnsan Hakları, Teknolojinin Hukuki Etkileri, Özel ve Ceza Hukuku Boyutuyla Bilişim Teknolojileri, Gibi Çeşitli Etkinlikler/Seminer/Çalıştay/Sempozyum/Panel	Bahçeşehir, Galatasaray, İbn Haldun, İstanbul Medeniyet, Kadir Has, MEF, Özyeğin, Trakya, Yalova
Siber Vatan	Siber Vatan Eğitimi/Ulusal Siber Güvenlik Stratejisi/Siber Vatan Programı	Afyon Kocatepe, Muğla Sıtkı Koçman, Trabzon
	Siber Vatan İş Birliği Protokolü	Batman, Kırıkkale, Manisa Celal Bayar
	Siber Vatan ve Siber Güvenlik Webinarı	Tarsus
	Siber Güvenlik ve Savunma	Bartın
	21. Yüzyılda Türkiye’nin Güvenliği Temalı Konferans	Kadir Has

	Ulusal Siber Güvenlik Çalıştayı	Gazi
	Siber Güvenlik ve Darbeler Konferansı	Adana Alparslan Türkeş Bilim ve Teknoloji
	Ufuk 2020 Güvenli Topluluklar Alanı 2019 Çağruları	Yıldız Teknik
	Dijital Türkiye Yapay Zekâ ve Siber Güvenlik	Erzincan Binalı Yıldırım
	Sanayide Yerli ve Milli Dönüşüm Paneli	İstanbul Sabahattin Zaim
	Kamuda Siber Güvenlik	Gazi, Gaziantep, İstanbul Sabahattin Zaim, Yıldız Teknik
	Dünyanın Kilidi: Dijital Kale Siber Güvenlik	İstanbul Sağlık ve Teknoloji
	Ülkelerin Kritik Altyapılarında Siber Güvenlik: Dijital Savaşın Bedeli	Özyeğin
	Uluslararası Anayurt Güvenliği Konferansı	Hasan Kalyoncu
	Akdeniz’de Güvenlik İstikrar ve İş Birliği Uluslararası Sempozyumu	Ankara Sosyal Bilimler
	Azerbaycan’da Siber Ekosistemin Oluşumu Konferansı/Yazılım Mühendisliği Bölüm Başkanının Katılımı Haberi	İstanbul Gelişim
	Azerbaycan ile Siber Güvenlik Alanında İş Birliği Görüşmesi	Sakarya
	Avrupa Siber Güvenlik Stratejileri ve Normatif Güç Olarak Avrupa Birliği	İzmir Kâtip Çelebi
	Dijital Avrupa Programı Bilgilendirme Toplantısı 2023	Acıbadem Mehmet Ali Aydınlar
Siber Güvenlik ve Yönetim Bilişim Sistemleri (YBS)	YBS Bölümünün Siber Güvenlik Alanındaki Yeri	Bandırma Onyediy Eylül
	Siber Güvenlik YBS Mezunlarına Emanet Edilmeli	İstanbul Medipol
	Siber Güvenlik Alanında YBS Mezun olarak Çalışmak	Karadeniz Teknik
	11. Uluslararası Yönetim Bilişim Sistemleri Kongresi/Rektör ve Öğrenci Katılım Haberi	Konya Gıda ve Tarım
Atölyeler	Siber Güvenlikte Yapay Zekâ	İstanbul
	Gelişim Atölyeleri	İstanbul Gelişim
Festivaller	Fırat Cyber Security Fest 2019	Fırat
	Bilişim Festivali IFEST 2023	Batman
	DEICY’24 Digital Economy, Internet of Things, Cybersecurity	İstanbul Kültür
Zirveler/Kongreler	Yönetim Bilişim Sistemleri Zirvesi IMISC2025	Konya Gıda ve Tarım
	Siber Güvenlik Zirvesi	İbn Haldun, İstanbul Nişantaşı, İstanbul Ticaret, Fırat, Süleyman Demirel
	2. Siber Güvenlik Zirvesi	Gazi
	6. Euritech Zirvesi	İstanbul Teknik
	7. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi/Akademisyenler Ödüllendirildi	İstanbul Gedik
	RaConf’24 Siber Güvenlikte Rakun Zirvesi	Sakarya

	Bilgisayar Mühendisliği Öğrencileri Kongresi BİLMÖK/Bilgisayar Klubü Öğrencilerinin Katılım Haberi	Kocaeli Sağlık ve Teknoloji
	11. Uluslararası Yönetim Bilişim Sistemleri Kongresi/Rektör ve Öğrenci Katılım Haberi	Konya Gıda ve Tarım
Çalıştaylar	Ulusal Siber Güvenlik Çalıştayı	Gazi
	1. Uluslararası Siber Güvenlik Çalıştayı ve Sertifika Programı	Ordu
	6. Uluslararası Siber Güvenlik Çalıştayı	İstanbul Gelişim
	III. Araştırma Grupları Çalıştayı	İstanbul/Cerrahpaşa
	Adli Bilişim ve Siber Güvenlik Eğitim Programlarına Yönelik Mevcut ve İhtiyaç Analizi Çalıştayı-Teknoloji Çalıştayları Serisi-2	İstanbul Ticaret
	Siber Zorbalık Konulu Çalıştay	Kastamonu Üniversitesi ile Kastamonu İl Milli Eğitim Müdürlüğü İşbirliği
	3. Ulusal Kripto Günleri Çalıştayı	Orta Doğu Teknik
	Bağlantılı Araçlardan Otonom Araçlara: Akıllı Ulaşım Sistemleri Çalıştayı	Marmara
Raporlar	Adli Bilişim ve Siber Güvenlik Eğitim Programlarına Yönelik Mevcut ve İhtiyaç Analizi Çalıştayı Raporu	İstanbul Ticaret
	Mobil İletişim Sektörü Raporu	İstanbul
İşletme Ziyaretleri/Teknik Geziler	Turkcell Siber Güvenlik Operasyon Merkezi	Beykoz
Ortaklıklar/İş Birliği Anlaşmaları	EC-Counil Academia (Lisans-Yüksek Lisans Eğitimi/İş Ortaklığı) Anlaşmaları	Işık
	EC-Counil Academia (Sertifikalı Eğitim Programı) Ortaklığı	Işık
	EC-Counil Academia (Siber Güvenlik Teknisyenliği Eğitimi/Beyaz Şapkalı Hacker Eğitimi) İş Birliği	Kocaeli Sağlık ve Teknoloji
	Cyber Exam Siber Güvenlik Laboratuvarı Ortaklık Programı Anlaşması (CyberPath A.Ş.İş Birliği)	İstanbul Ticaret
	Siber Tatbikat Platformu Ürünü Geliştirilmesi (Cyrops Siber Güvenlik A.Ş. ile STM A.Ş. İş Birliği)	Zonguldak Bülent Ecevit
	İstanbul Emniyet Müdürlüğü'nde Görevli Personelin Siber Güvenlik Tezsiz Yüksek Lisans Eğitimi Yapmasına Yönelik İş Birliği Protokolü	Marmara
	“Warning” Kod Adlı Araştırma Projesi	Kadir Has
	Siber Akademi	İstanbul Gelişim
Projeler	Dijital İkiz	İstanbul Teknik
	Secure Future	İstanbul Ticaret
	İstanbul Adli Bilişim Laboratuvarı	İstanbul Ticaret
	She 4Cyber/Akademisyene Hibe Projesi Desteği	Kadir Has
	Bölgesel Kalkınma Odaklı Misyon Farklılaşması ve İhtisaslaşma	Kırklareli
	Cisco Academy İçin Cisco Eğitmen Eğitimi Teknik Destek	Kırklareli

	Siber Güvenlik Uzmanı Yetiştirme Projesi	Akdeniz
	Blokzincir Teknolojileri ve İnovasyon Merkezi Açılışı	İstanbul
	Ülkemizin İlk Siber Koza İnovasyon Merkezi Açılışı	İstanbul/Cerrahpaşa
	Bilişim Teknolojileri ve Eğitim Merkezi Kurulacağı Duyurusu	İstanbul Sabahattin Zaim
Merkezler	Sürekli Eğitim Merkezi ile Zeytinburnu Belediyesi Eğitim Protokolü	İstanbul Ticaret
	Siber Güvenlik Uygulama ve Araştırma Merkezi Kurulacağı Duyurusu	Kayseri
	Siber Güvenlik ve Kritik Altyapı Koruma Uygulama ve Araştırma Merkezine TÜBİTAK Desteği Duyurusu	Kadir Has
	Siber Güvenlik Uygulama ve Araştırma Merkezi'nin Hayata Geçirilişi	Nevşehir Hacı Bektaş Veli
	Siber Güvenlik Kampı	Kadir Has
	Siber Güvenlik Lisesi Açılışı	İstanbul/Cerrahpaşa
Liselere/12. Sınıflara/Mezunlara Yönelik Etkinlikler	Teknopark İstanbul'da Türkiye'nin İlk Siber Güvenlik Meslek ve Teknik Anadolu Lisesi Açılışı	İstanbul Ticaret
	Gelecek Yıllarda Lise Düzeyinde Siber Güvenlik Sertifika Eğitimi Verilmesi Düşüncesi	Manisa Celal Bayar Üniversitesi ile Zafer Kalkınma Ajansı İşbirliği
	Siber Güvenlik Eğitiminin Ortaokulda Başlaması Gerekliği Düşüncesiyle RaConf24 Siber Güvenlikte Rakun Zirvesi'nde Lise Öğrencilerine Katılma İmkânı Vermesi	Sakarya
Toplumun Farklı Kesimlerine Yönelik Siber Güvenlik Eğitimi	Bilişim Teknolojileri Eğitim Merkezi Kurularak En Az 1 Yıl Herhangi Bir İşte Çalışmayanlar ve Öğrenci Olmayanlara Yönelik Eğitim Verilmesi	İstanbul Sabahattin Zaim
	Ne Eğitimde Ne İstihdamda Olan Gençler İçin Eğitim	Sivas Cumhuriyet
	Zeytinburnu'da Yaşayan 16-35 Yaş Aralığında Herkesin Katılabileceği Eğitim	İstanbul Ticaret Üniversitesi (Sürekli Eğitim Merkezi), Zeytinburnu Belediyesi ve Siber Güvenlik Teşkilatı Protokolü
	KOBİ'lerin Siber Farkındalığının Artırılması	İstanbul Ticaret

Not. 208 Üniversitenin internet sitesindeki “duyurular”, “haberler”, “etkinlikler”, gibi başlıklar altında kamuoyuna yapılan paylaşımlarından site içi arama yapılarak veriler elde edilmiştir. Site 01.08.2024-25.09.2024 tarihleri arasında güncel ve geçmişe yönelik olarak taranmıştır. Toplanan veriler kategorize edilerek tablo (yazar tarafından) oluşturulmuştur.

Tablo 1.'de gösterildiği üzere üniversitelerimiz siber güvenlik konulu farkındalık eğitimleri, kariyer fırsatları, burs ve iş imkânları, sertifika programları, uygulamalı eğitimler, kamplar ve yaz/kış okulları, atölyeler, teknik geziler, festivaller, zirveler, çalıştaylar, raporlar, projeler, iş ortaklıkları anlaşmaları gibi pek çok muazzam işe imza atmıştır. Ayrıca üniversitelerimiz siber güvenliği siber vatan ve siber hukuk boyutuyla da ele almıştır.

Üniversitelerin siber güvenlik konusundaki muazzam çabası şu şekilde özetlenebilir:

- Siber güvenlik faaliyetleri içerisinde en çok gerçekleştirilen faaliyetler sıralanırsa “siber güvenlik tanıtım ve farkındalık faaliyeti” 52 üniversite ile birinci, “siber güvenlik ve kariyer fırsatları” 29 üniversite ile ikinci, “siber vatan” ise 23 üniversite ile üçüncü olmuştur.
- Üniversitelerimiz sadece üniversite öğrencilerinin ufkunu açmak, onları yetiştirmek, akademik/ıdari personeli bilgilendirmekle sınırlı kalmamış, liselere ve toplumun farklı kesimlerine, KOBİ (Küçük ve Orta Büyüklükteki İşletmeler)’lere de siber güvenlik eğitimi verilmesi konusunda öncülük etmiştir.
- Faaliyetlerde konunun tüm muhatapları akademisyenler, öğrenciler, mezunlar, idari personeller, güvenlik güçleri çalışanları, il milli eğitim müdürlüğü, özel sektör kuruluşu temsilcileri, uluslararası kurumları bir araya gelmiştir.
- Özellikle il emniyet müdürlükleri ve il jandarma komutanlıklarında siber suçlarla görevli birim personelinin farkındalık eğitimine katılması çok kıymetlidir. Katılımcılara birinci ağızdan siber güvenlik, siber suç, siber zorbalık, siber tehditler, siber olaylarla mücadele anlatılmıştır. Güvenlik güçleri aracılığıyla bu bilgilendirme/bilinçlendirme faaliyetlerinin yapılması konunun ne kadar önemli olduğunun ortaya konulması ve katılımcılar üzerinde oluşturacağı etki açısından değerlidir.
- Üniversite-güvenlik güçleri işbirliği bazen bir eğitim programı anlaşmasıyla sonuçlanmıştır. Bu durum, güvenlik güçleri personelinin siber güvenlik alanındaki saha tecrübesini akademiye aktarması/taşıması açısından oldukça değerlidir.
- Üniversite-özel sektör iş birliği içerisinde özellikle siber güvenlik alanındaki öncü firmaların sahiplerinin kariyer yolculuklarını anlatmaları bu alana ilgi duyanlar açısından bir rehber niteliğindedir. Sektörün ileri gelen firmalarının başarılı öğrenciler için kariyer fırsatları (iş imkânı) ve burs imkânı sağlaması da oldukça önemlidir.
- Bir üniversite, yabancı üniversitelerle uluslararası yüksek lisans eğitim protokolü imzalamıştır. Protokol gereği, öğrenci akademik eğitiminin belirli bir süresini kendi üniversitesinde; kalan kısmını yurtdışındaki anlaşmalı üniversitede öğrenim görerek tamamlayacaktır. Bu durum, öğrencilerin hem Türkiye’de hem de uluslararası platformlarda yarışabilecek bir şekilde yetiştirilmesi açısından eşsiz bir imkândır.
- Siber güvenlik eğitimleri sertifikalı, uygulamalı eğitimler, kamplar, yaz-kış okulları gibi gruplar tarafından temsil edilmekle birlikte eğitimlerin bazıları ücretli, bazıları ücretsiz olarak sunulmuştur. Ücretsiz imkânların sunulmuş olması maddi açıdan dezavantajlı grupların da bu eğitimlerden faydalanabilmesi açısından bir fırsat niteliğindedir.
- Kimi zaman üniversiteler, kendileri düzenlemese de, başka kurum/kuruluşların siber güvenlik konulu etkinliklerini de paylaşılarak (Uşak Üniversitesi, Malatya Turgut Özal Üniversitesi gibi) ya da bu etkinliklere katılarak siber güvenlik faaliyetlerine bu yönüyle de katkı sağlamıştır.
- Bazı üniversiteler her yıl siber güvenlik faaliyeti gerçekleştirme yönünde hareket etmişken bazıları bir tek faaliyetle sınırlı kalmıştır.

Türkiye’de “Siber Güvenlik” Programları ve Siber Güvenlik Müfredatlarının Durumu

Türkiye’deki Üniversitelerin Siber Güvenlik Programları

Türkiye’de “siber güvenlik” adıyla açılan ön lisans programları YÖK Önlisans Atlası, lisans programları YÖK Lisans Atlası kullanılarak; yüksek lisans ve doktora programları ise 208 üniversitenin enstitü sayfaları taranarak tespit edilmiştir. Türkiye’de 208 üniversitenin 22’sinde (22/208 =) % 10,57’sinde “siber güvenlik” programı açılmıştır. Siber güvenlik programları Tablo 2.’de sunulmuştur.

Tablo 2. Türkiye'deki Üniversitelerde "Siber Güvenlik" Programları

Sıra No	Üniversite Adı	İl	Üniversite Türü	Siber Güvenlik Program Türleri			
				Ön Lisans	Lisans	Yüksek Lisans	Doktora
1	Adana Alparslan Türkeş Bilim ve Teknoloji	Adana	Devlet			√	
2	Ankara	Ankara	Devlet	√			
3	Antalya Bilim	Antalya	Vakıf			√	
4	Bahçeşehir	İstanbul	Vakıf			√	
5	Düzce	Düzce	Devlet			√	
6	Ege	İzmir	Devlet	√			
7	Gebze Teknik	Kocaeli	Devlet	√		√	
8	Işık	İstanbul	Vakıf			√	
9	İnönü	Malatya	Devlet			√	
10	İstanbul/Cerrahpaşa	İstanbul	Devlet			√	
11	İstanbul Aydın	İstanbul	Vakıf			√	
12	İstanbul Teknik	İstanbul	Devlet	√	√		
13	İstanbul Ticaret	İstanbul	Vakıf	√		√	√
14	İstinye	İstanbul	Vakıf			√	
15	Kadir Has	İstanbul	Vakıf			√	
16	Kayseri	Kayseri	Devlet			√	
17	Koç	İstanbul	Vakıf			√	
18	Marmara	İstanbul	Devlet			√	
19	Orta Doğu Teknik	Ankara	Devlet			√	
20	Sabancı	İstanbul	Vakıf			√	√
21	Üsküdar	İstanbul	Vakıf			√	
22	Yıldız Teknik	İstanbul	Devlet			√	
Toplam Program Sayısı				5	1	19	2

Not. Verilen YÖK Önlisans-Lisans Atlası ve üniversitelerin enstitüler sayfasından (01.08.2024-25.09.2024 tarihleri arasında tarama yapılarak) elde edilmiştir. Tablo yazar tarafından oluşturulmuştur.

Tablo 2.'de gösterildiği üzere, Türkiye'de 22 üniversitede siber güvenlik eğitimi verilmektedir ve bunların 13'ü İstanbul'da yer almaktadır. Dolayısıyla İstanbul, siber güvenlik eğitiminin merkezi konumundadır. 22 üniversitenin 12'si devlet, 10'u vakıf üniversitesi statüsündedir. Bu açıdan siber güvenlik programları daha çok devlet üniversitelerinde açılmıştır. Türkiye'deki siber güvenlik programlarının, 5'i ön lisans, 1'i lisans, 19'u yüksek lisans ve 2'si doktora düzeyinde eğitim vermektedir. Siber güvenlik ön lisans programlarının 4'ü devlet, 1'i vakıf; siber güvenlik lisans programlarının tamamı devlet; yüksek lisans programlarının 9'u devlet, 10'u vakıf; doktora programlarının tamamı vakıf üniversitesi bünyesinde açılmıştır. En çok yüksek lisans düzeyinde siber güvenlik programı açılmıştır. Sebebi kesin olarak bilinmemekle birlikte, bu alandaki akademisyen ihtiyacının karşılanabilmesi amacıyla yüksek lisans programlarının açılmasına ağırlık verildiği düşünülmüştür. İstanbul Ticaret Üniversitesi'nde ön lisans, yüksek lisans ve doktora; İstanbul Teknik Üniversitesi'nde ön lisans ve lisans; Gebze Teknik Üniversitesi'nde ön lisans ve yüksek lisans; Sabancı Üniversitesi'nde yüksek lisans ve doktora programları mevcuttur. Üniversitenin bir alanda ve farklı düzeylerde eğitim hizmeti sunması, her kademede nitelikli iş gücünün yetiştirilmesi açısından oldukça değerlidir. Bu anlamda 3 farklı kademede siber güvenlik programı açan tek üniversite İstanbul Ticaret Üniversitesi'dir. Siber güvenlik ön lisans ve lisans eğitiminde devlet; lisansüstü eğitimde vakıf üniversiteleri ön plandadır. Doktora düzeyinde eğitim veren bir devlet üniversitesi bulunmamaktadır.

Siber Güvenlik Müfredatlarının Durumu

Siber güvenlik eğitimi veren 22 üniversitenin tüm eğitim düzeylerindeki ders katalogları incelemiştir. Sabancı Üniversitesi'nin doktora, Yıldız Teknik Üniversitesi'nin yüksek lisans ders müfredatına ulaşamamıştır. Fen bilimlerinde konumlandırılan siber güvenliğin, temel kategorilerinin saptanması (büyük resmi görebilmek) için tüm ders katalogları birleştirilmiştir. 600'ü aşkın siber güvenlikle ilgili ders, isim ve konu benzerlikleri açısından

sınıflandırılmıştır. Toplamda 24 kategori elde edilmiştir. Sadece siber güvenlik müfredatlarının kategorizasyonu Tablo 3.’te sunulmuştur.

Tablo 3. Siber Güvenlik Müfredatlarının Kategorizasyonu

Siber Güvenlik Müfredatlarındaki Ders Kategorilerinin İsimleri			
Bilgisayar	Nesnelerin İnterneti	Veri ve Veri Güvenliği	Sızma Testi
İnternet	Blok Zincir	Büyük Veri Güvenliği	Siber Güvenlik
Web	Yapay Zekâ	Veri Madenciliği	Adli Bilişim
Ağ	Makine Öğrenmesi	Diğer Dijital Dönüşüm	Etik
Algoritmalar	Bulut Bilişim	Şifreleme	Hukuk
Kuram/Teoriler	Bilgi Güvenliği	Kötü Amaçlı Yazılımlar	Diğer

Not. Veriler Türkiye’de siber güvenlik eğitimi veren 22 üniversitenin (01.08.2024-25.09.2024 tarihleri arasında) internet sitesindeki “Ders Katalogları”ndan elde edilmiştir ve kataloglar Microsoft Excel’de işlenerek tablo (yazar tarafından) oluşturulmuştur.

Tablo 3’e göre ders kataloglarında siber güvenlik eğitimi teknik yönü, dijital dönüşüm yönü ve hukuki yönü dikkate alınarak hazırlanmıştır. Siber güvenlik eğitiminin teknik yönünü bilgisayar, internet, web, ağlar, algoritmalar, kötü amaçlı yazılımlar, sızma testleri, şifreleme; siber güvenlik eğitiminin dijital dönüşüm yönünü nesnelerin interneti, blok zincir, yapay zekâ, makine öğrenmesi, bulut bilişim, veri madenciliği; siber güvenlik eğitiminin hukuki yönünü adli bilişim, etik, hukuk gibi dersler oluşturmaktadır. Ayrıca her bir kategori içerisinde yer alan dersler açısından bir sıralama yapılacak olursa, en fazla ders siber güvenlik kategorisindedir. Bunu bilgisayar kategorisi ve ağ kategorisi takip etmiştir. Siber güvenlik kategorisinde yer alan derslerin isimleri Tablo 4.’te sunulmuştur.

Tablo 4. Siber Güvenlik Kategorisinde Yer Alan Dersler

Siber Veri Analitiği	Siber Güvenlik İçin Linux Temelleri	Siber Güvenlik Mühendisliklerinde Stokastik Analiz	Siber Savaş ve Güvenlik	Endüstri 4.0 İçin Siber Güvenlik: Tasarım ve İmalat Analizi
Siber Sistemler ve Bilgi Güvenliği	Siber Güvenlikte Elektromanyetiğin Önemi	Siber Saldırı Teknikleri	Stratejik Siber Güvenlik	Siber Güvenlik İçin Veri Madenciliği
Siber Dayanıklılık	Siber Güvenlik Operasyonları	Siber Saldırı Teknikleri ve Savunma Teknolojileri	Siber Güvenlik Hukuku	Siber Güvenlik İçin Yapay Zekâ
Siber Fiziksel Sistemlerde İnsan Faktörü	Siber Güvenlik Mühendisliğinde Tasarım-I	Siber Savunma Teknikleri ve Kontrol Mekanizmaları	Siber Güvenlik ve Veri Gizliliği Hukuku	Siber Güvenlikte Yapay Zekâ
Siber Güvenlik	Siber Güvenlik Mühendisliğinde Tasarım-II	Siber Saldırı ve Savunma Yöntemleri-I	Siber Güvenliğin Hukuki Boyutları	Siber Güvenlikte Yapay Zekâ Uygulamaları
Siber Güvenliğe Giriş	Siber Güvenlik ve Yönetimi	Siber Saldırı ve Savunma Yöntemleri-II	Siber Güvenliğin Yasal Boyutları	Yapay Zekâ ve Siber Güvenlik
Siber Güvenlik Temelleri	Siber Güvenlik Planlama ve Yönetimi	Siber Güvenlik, Saldırı ve Savunma Yöntemleri	Siber Güvenliğin Yasal Yönleri	IoT ve Siber Güvenlik
Siber Güvenliğin Temelleri	Siber Güvenlik Planlaması ve Yönetimi	Siber Olay Yönetimi	Siber Güvenlik: Etik Kurallar, Kanunlar ve İnsan Etkisi	Nesnelerin İnternetinde Siber Güvenlik

Siber Güvenlik İçin Temeller	Siber Güvenlik Yönetimi	SOME Ekibi Uygulamaları	Siber Güvenlikte Araştırma Yöntemleri	Bulut Bilişimde Siber Güvenlik
Siber Güvenlik Başlangıç-1	Siber Güvenlik Yönetimi	Siber Güvenlikte Saha Uygulaması	Siber Güvenlikte Araştırma Yöntemleri, Değerlendirme ve Yaygınlaştırma Etiği	Siber Güvenlik İçin Makine Öğrenmesi Yöntemleri
Siber Güvenlik Başlangıç-II	Siber Güvenlik Yönetimi Düzenlemeleri ve Uyum	Sayısal Adli İşlemler ve Siber Saldırlara İlk Müdahale	Siber Güvenlikte Araştırma Yöntemleri ve Etik	Siber Güvenlik İçin Makine Öğrenmesi Tasarımı ve Uygulaması
Siber Güvenlik İçin Betik Diller	Siber Güvenlik Yönetimi Projesi	Siber Adli Bilişim	Siber Güvenlikte Özel Konular	Siber Güvenlikte Derin Öğrenme Uygulamaları
Siber Güvenlik İçin Kodlama Dilleri	Siber Güvenlikte Kimlik Doğrulama	Siber Savaş	Siber Güvenlikte İleri Teknolojiler	Web ve Siber Güvenlik
Siber Güvenlik İçin Komut Dosyası Dilleri	Siber Güvenlikte Sosyal Mühendislik	Siber Güvenlik ve Siber Savaş	Endüstride Siber Güvenlik	Dijital Güvenlik ve Kimlik

Not. Veriler siber güvenlik bölümü olan 22 üniversitenin internet sitesindeki “Ders Katalogları”ndan elde edilmiştir. Tablo yazar tarafından oluşturulmuştur.

Tablo 4.’e göre siber güvenlik kategorisi, toplam 70 farklı ders ismi ile temsil edilmiştir.

Türkiye’de fen bilimleri alanında konumlandırılan siber güvenlik programlarından elde edilen bulgular aşağıda sıralanmıştır:

- Siber güvenlik programlarında, “siber güvenlik kategorisi” derslerinde salt bir siber güvenlikten bahsetmek mümkün değildir. Siber güvenlik müfredatları sadece teknik altyapısı düşünülerek oluşturulmamıştır.
- Siber güvenlik tanım, tasarım, planlama, yönetim boyutuyla ele alındığı gibi siber tehdit (sosyal mühendislik), savunma, siber olaylara müdahale boyutuyla da ele alınmıştır. Hatta siber güvenliğin sınırlar ötesi boyutu (savaş) da düşünülerek müfredatlar hazırlanmıştır.
- Endüstri 4.0 ile hayatımıza giren bulut bilişim, yapay zekâ, nesnelerin interneti, veri madenciliği, makine öğrenmesi gibi dersler tüm yönleriyle müfredatlar da yerini almıştır. Bir başka deyişle, dijital dönüşüm ile siber güvenlik arasındaki bağ kurulmuştur. Sadece bulut bilişim anlatılmamış, bulut bilişimde siber güvenlik nasıl olmalıdır sorusuna cevap bulunabilecek zenginlikte müfredatlar oluşturulmuştur.
- Müfredatlar siber güvenliğin etik boyutu düşünülerek tasarlanmıştır. Siber tehditler ve siber saldırılar etik zafiyetlerden kaynaklanmaktadır. Bu bilinç, ön lisans, yüksek lisans ve doktora programlarının müfredatlarında “bilişim etiği”, “siber güvenlik: etik kurallar, kanunlar ve insan etkisi”, “siber güvenlikte araştırma yöntemleri ve etik”, “siber güvenlikte araştırma yöntemleri, değerlendirme ve yaygınlaştırma etiği”, “etik güvenlik kırmaya giriş” ve “etik korsanlık (etik ihlaller)” gibi çeşitli isimlerdeki derslerle verilmektedir. Siber güvenlik (mühendisliği) lisans programının seçmeli dersler listesi verilmediği için lisans düzeyindeki durumu bilinmemektedir.
- Siber güvenliğin hukuki boyutu düşünülmüştür. Ön lisans ve lisansüstü eğitim müfredatlarında “adli bilişim teknikleri ve hukuku”, “bilişim hukuku”, “siber güvenlik hukuku”, “siber güvenlik ve veri gizliliği hukuku”, “siber güvenlik: etik kurallar, kanunlar ve insan etkisi”, “siber güvenliğin hukuki boyutları/yasal boyutları/yasal yönleri”, “güvenliğin sosyal, ekonomik ve hukuki yönleri”, “güvenlik, hukuk ve ahlâk”, “fıkri mülkiyet hakları” ve “insan hakları hukuku” gibi dersler bulunmaktadır.
- Siber hukuk derslerinin içerikleri incelendiğinde ise Fikri Mülkiyet Kanunu, Elektronik İmza Kanunu, Elektronik Haberleşme Kanunu, Elektronik Ticaret Kanunu, Kişisel Verilerin Korunması Kanunu (KVKK), Bilişim Hukuku, Türk Ceza Kanunu, Türk Ceza Muhakeme Kanunu gibi ulusal düzenlemeler ile Avrupa Birliği Genel Veri Koruma Tüzüğü (CDPR), Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası-HIPAA gibi uluslararası düzenlemelerin ele alındığı görülmüştür.

Türkiye’de Sosyal Bilimler Alanında Siber Güvenlik Eğitiminin Durumu

Sosyal Bilimlerde Siber Güvenlik: Muhasebe ve Finans Yönetimi Lisans Programları

Türkiye’de “Muhasebe ve Finans Yönetimi” bölümleri YÖK Lisans Atlası kullanılarak tespit edilmiştir. Ülkemize 14 ilde, 15 üniversitede, 15 program bulunmaktadır. Muhasebe eğitimi veren üniversitelerin 12’si devlet, 3’ü vakıf üniversitesi statüsündedir. Sosyal bilimlerde – “Muhasebe ve Finans Yönetimi” bölümünde siber güvenliğin durumu Tablo 5.’te sunulmuştur.

Tablo 5. Sosyal Bilimlerde Siber Güvenlik - Muhasebe ve Finans Yönetimi Lisans Müfredatlarının Durumu

Üniversite Adı	“Siber Güvenlik” adı ile açılan bir ders var mıdır?	Siber Güvenlik ile ilişkili içerik taşıyan dersler var mıdır?	“Siber Hukuk” adı ile açılan bir ders var mıdır?	Siber Hukuk-Etik ile ilişkili içerik taşıyan dersler var mıdır?
Afyon Kocatepe				
Burdur Mehmet Akif Ersoy				
Isparta Uygulamalı Bilimler				
Kayseri				
Kırklareli				
Necmettin Erbakan				
İstanbul Aydın (V) ⁷	Siber Güvenlik			
Başkent (V)		Bilgisayar Okuryazarlığı Bilgi Güvenliği Denetimde Üçlü Savunma Hattı Yapay Zekâ Uygulamaları Veri Madenciliği Blokzincir		Verimlilik Artırıcı Yaklaşımlar ve Teknikler Bilgi Güvenliği
İstanbul Arel (V)		Dijital Okuryazarlık CS50X Kodluyoruz		
Kütahya Dumlupınar		Bilişim Sistemleri Teknolojileri		
Uşak		Bilişim Teknolojileri		Bilişim Teknolojileri
Bilecik Şeyh Edebali		Temel Bilgi Teknolojisi Kullanımı Blok Zincir ve Kripto Varlıklar		Temel Bilgi Teknolojisi Kullanımı
Muğla Sıtkı Koçman		Bilgisayar Kullanımı İş İstihbaratı Algoritma ve Programlama Temelleri		
Malatya Turgut Özal		Dijital Dönüşüm Veri Madenciliği		
Trakya		Bilgi Sistemleri ve Teknolojileri-I Bilgi Sistemleri ve Teknolojileri-II Veri Madenciliği		

Not. Veriler “Muhasebe ve Finans Yönetimi” programı olan üniversitelerin (01.08.2024-25.09.2024 tarihleri arasında) internet sitesindeki “Ders Katalogları”ndan elde edilmiştir ve kataloglardaki dersler isim ve içerik açısından incelenmiş ve tablo (yazar tarafından) oluşturulmuştur.

⁷ (V): Vakıf üniversitelerini belirtmek için kullanılmıştır.

Tablo 5.'e göre Türkiye'de muhasebe lisans düzeyinde eğitim veren 15 üniversitenin 6'sında siber güvenlik ve siber hukuk ya da bunlarla ilişkili derslere rastlanmamıştır. Siber güvenlik adıyla müfredatında ders olan tek üniversite İstanbul Aydın Üniversitesi'dir. Siber güvenlik ile ilişkili dersler açısından en zengin müfredat Başkent Üniversitesi'ndedir. 15 üniversitenin müfredatında siber hukuk adıyla açılan bir derse rastlanmamıştır. Siber hukuk ve etik ile ilişki dersler açısından Başkent Üniversitesi, Uşak Üniversitesi ve Bilecik Şeyh Edebali Üniversitesi'nin müfredatında derse rastlanmıştır.

İstanbul Aydın Üniversitesi'nin müfredatında yer alan “siber güvenlik” dersi, “üniversite seçmeli ders”idir. Bundan dolayı dersin ilgili yarıyılta açılıp açılmadığı bilinmemektedir. Siber hukukla ilişkilendirilen dersler fen bilimlerindeki programlarda olduğu gibi zengin bir içeriğe sahip değildir. Bilecik Şeyh Edebali Üniversitesi'nin “Temel Bilgi Teknolojileri Kullanımı” dersinin sadece 14. haftasında KVKK, internet kanunu, bilişim suçları, bilişim etiği ve telif hakları işleneceği görülmektedir (ebs.bilecik.edu.tr). Fen bilimleri alanında dönemlik olarak siber hukuk dersi açılırken, muhasebe lisans programlarında konunun tek bir haftaya sığdırılması, siber güvenlik konusunun öneminin yeterince anlaşılmadığını göstermektedir. Fen bilimleri alanında, dijital dönüşüm ile siber güvenlik bağı kurulmuşken, sosyal bilimlerde (muhasebede) bu bağın kurulamadığı belirlenmiştir. Ayrıca muhasebe ders kataloglarında siber güvenliğin teknik boyutu (bilgisayar, internet, ağlar, algoritmalar, sızma testi, şifreleme gibi) sınırlı düzeyde ele alınmıştır.

Sosyal Bilimlerde Siber Güvenlik: Bankacılık Lisans Programları

Türkiye'de “Bankacılık”, “Bankacılık ve Finans”, “Bankacılık ve Sigortacılık” ve “Finans ve Bankacılık” adı altında açılan programlar YÖK Lisans Atlası kullanılarak tespit edilmiştir. Ülkemize 33 ilde, 41 üniversitede, 45 bankacılık programı bulunmaktadır. Bankacılık lisans eğitimi veren üniversitelerin 35'i devlet, 6'sı vakıf üniversitesi statüsündedir. Bankacılık eğitimi veren 45 programdan 2'sinin müfredatına ulaşılamadığından 43 program incelenmiştir. Bazı üniversitelerin teknoloji içerikli bazılarının ise siber güvenlik içerikli dersinin olmadığını gösteren veriler Tablo 6.'da sunulmuştur.

Tablo 6. Bankacılık Müfredatlarında Teknoloji/Bilgisayar ve Siber Güvenlik/Siber Hukuk Dersi Olmayan Üniversiteler

Kriterler	Kriteri Sağlayan Üniversite Sayısı	Üniversite Adı
Bilgisayar ve Teknoloji İçerikli Dersi Olmayan Üniversiteler	3	Zonguldak Bülent Ecevit, Karabük, Kastamonu
Siber Güvenlik ve Siber Hukuk İçerikli Dersi Olmayan Üniversiteler	18	Zonguldak Bülent Ecevit, Karabük, Kastamonu, Afyon Kocatepe, Isparta Uygulamalı Bilimler, Tokat Gaziosmanpaşa, Karamanoglu Mehmetbey, Trakya-Uygulamalı Bilimler Fakültesi, Ankara Yıldırım Beyazıt-İşletme Fakültesi, Ankara Yıldırım Beyazıt-Şereflikoçhisar Uygulamalı Bilimler Fakültesi, Çankırı Karatekin, Kütahya Dumlupınar, Manisa Celal Bayar, Necmettin Erbakan, Nevşehir Hacı Bektaş, Sivas Cumhuriyet, Giresun, Kahramanmaraş Sütçü İmam

Not. Veriler bankacılık programı olan üniversitelerin (01.08.2024-25.09.2024 tarihleri arasında) internet sitesindeki “Ders Katalogları”ndan elde edilmiştir ve kataloglardaki dersler isim ve içerik açısından incelenmiş ve tablo (yazar tarafından) oluşturulmuştur.

Tablo 6.'ya göre Türkiye'de bankacılık lisans düzeyinde eğitim veren 3 üniversitede bilgisayar ve teknoloji içerikli hiç ders bulunmazken, 18 üniversitede siber güvenlik ve siber hukuk içerikli hiç ders bulunmamaktadır. Dijital çağda bilgisayar/teknoloji içerikli derslerin dahi müfredatlar olmaması şaşırtıcıdır. Diğer bankacılık bölümlerine ilişkin veriler Tablo 7.'de sunulmuştur.

Tablo 7. Sosyal Bilimlerde Siber Güvenlik - Bankacılık Müfredatlarının Durumu

Üniversite Adı	“Siber Güvenlik” adı ile açılan bir ders var mıdır?	Siber Güvenlik ile ilişkili içerik taşıyan dersler var mıdır?	“Siber Hukuk” adı ile açılan bir ders var mıdır?	Siber Hukuk-Etik ile ilişkili içerik taşıyan dersler var mıdır?	Diğer hukuk dersleri içerisinde siber hukuk ilişkisi kurulan bir ders var mıdır?
Erzincan Binali Yıldırım	Siber Güvenlik	Siber Güvenlik Modern Bilişim Teknolojileri Teknoloji Okuryazarlığı Robotik Kodlama Python Programlama Bilgi Güvenliği Siber Güvenlik		Siber Güvenlik Teknoloji Okuryazarlığı Bilgi Güvenliği	
İstanbul Nişantaşı (V)	Siber Güvenlik	Yapay Zekâ ve Kontrol Büyük Veri Endüstri 4.0 ve Dijital Dönüşüm Bilişim Teknolojileri Bilgisayar Programlamaya Giriş			
Ankara Hacı Bayram Veli (Finansal Bilimler Fakültesi)		Finans İçin Temel Programlama Teknolojik Gelişmeler Işığında Para ve Finans Sistemleri İnsan Bilgisayar Etkileşimi ve Arayüz Tasarımı Problem Çözme ve Algoritma Python Programlama Bilgisayar Ağları Ağ Yönetimi ve Güvenliği Bulut Bilişim Yeni Medya ve Dijital Dönüşüm Yeni Medya ve Veri Madenciliği Dijital Okuryazarlık Python Programlamaya Giriş Python Programlama Uygulamaları Endüstri 4.0 ve Dijital Dönüşüm Algoritma ve Puanlamaya Giriş Kripto Paralar, Blokzincir ve Akıllı Teknolojiler Bilişim Teknolojileri Yapay Zekâ Uygulamaları Arduino ile Robotik Kodlama Blok Tabanlı Kodlama Kripto Varlıklar Finansta Yapay Zekâ Uygulamaları	Bilişim Teknolojileri	Fikri ve Sınai Mülkiyet Hakları	
İstanbul Gelişim (V)					
Atatürk					
Burdur Mehmet Akif Ersoy					
Süleyman Demirel					

	Dijital Muhasebe ve Raporlama	
	Kripto Paralar ve Blockchain'e Giriş	
	Algoritmik Ticaret	
	Finansal Teknolojiler	
	Dijital Dönüşüm Ekosistemi	
	Dijital Dönüşüm ve Endüstri 4.0	
Tarsus	Veri Madenciliği	
	Finansal Teknolojiler	
	Algoritma ve Programlama	
	Blok Zincir Teknolojileri ve Sanal Para	
İstanbul Beykent (V)	Yapay Zekâ ve Veri Yönetimi	
	Yeni Trendlerin Finansal Sistem Etkileri	
	Bilgi ve Veri Okuryazarlığı	
İstanbul Arel (V)	Veri Bilimine Giriş	
	Dijital Okuryazarlık	
	CS50X Kodluyoruz	
Akdeniz	Yapay Zekânın Finansal Uygulaması	
	Veri Madenciliğine Giriş	
Çanakkale	Dijital Finans	
Onsekiz Mart	Temel Programlama	
	Blokzincir ve Finans	
Hitit	Teknolojileri	
	Temel Bilgisayar	
	Teknolojileri ve Kullanımı-II	
İstanbul Ticaret (V)	Makine Öğrenmesine Giriş	
	Yapay Zekâ Uygulamalarında	
	Temel Kavramlar	
Niğde Ömer Halisdemir	Temel Bilgisayar	
	Robotik Kodlama	
	Yapay Zekâ ve Veri Yönetimi	
Recep Tayyip Erdoğan	Kripto Paralar ve Blok Zincir Teknolojileri	
Uşak	Bilişim Teknolojileri Programlama Dilleri	Bilişim Teknolojileri
Balıkesir	Bilgi Teknolojileri	
Bilecik Şeyh Edebali	Temel Bilgi Teknolojisi Kullanımı	Temel Bilgi Teknolojisi Kullanımı
Bolu Abant İzzet Baysal	Blockchain Teknolojisi ve Kripto Para	
Kırklareli	Python Programlama	
Marmara	Bilgi Güvenliği Yönetimi	
Sivas Cumhuriyet	Dijital Para Sistemleri	
Trakya-Uzun Köprü	Veri Madenciliği	
Trakya- Keşan		
Yusuf Çapraz		Bilişim Etiği

Not. Veriler bankacılık bölümü olan üniversitelerin (01.08.2024-25.09.2024 tarihleri arasında) internet sitesindeki “Ders Katalogları”ndan elde edilmiştir ve kataloglardaki dersler isim ve içerik açısından incelenmiş ve tablo (yazar tarafından) oluşturulmuştur.

Tablo 7.’ye göre Bankacılık programlarında “siber güvenlik” adı altında (seçmeli) bir derse Erzincan Binali Yıldırım Üniversitesi ve İstanbul Nişantaşı Üniversitesi’nin müfredatında rastlanmıştır. Seçmeli ders niteliğinde olması sebebiyle dersin ilgili yarıyıldan açılıp açılmadığı bilinmemektedir. Siber güvenlik ile ilişkili dersler açısından en zengin müfredat İstanbul Gelişim Üniversitesi’ndedir. Bankacılık müfredatlarında siber hukuk dersi yoktur. Sadece 5 üniversitenin müfredatında siber hukuk ile ilişkili derse rastlanmıştır. Ayrıca bankacılık müfredatlarında yer alan pek çok hukuk dersi içerisinde Fikrî ve Sınai Mülkiyet Hakları isimli ayrı bir ders sadece Ankara Hacı Bayram Veli Üniversitesi’nde vardır. Bilecik Şeyh Edebali Üniversitesi’nin “Temel Bilgi Teknolojileri Kullanımı” dersinin sadece bir haftasında siber hukukun işleneceği gözükmemektedir. Trakya Üniversitesi’ndeki “Bilişim Etiği” dersinin ismi ile içeriği uyumsuzdur. Siber hukukla ilişkilendirilen dersler fen bilimlerindeki gibi zengin değildir. Fen bilimleri alanında önemlilik olarak siber hukuk dersi açılırken, bankacılık programlarında konunun tek bir haftaya sığdırılması ya da yüzeysel ele alınması, siber güvenlik konusunun önemini yeterince anlaşılmadığını göstermektedir. Yapay zekâ, büyük veri, veri madenciliği, blok zincir, bulut bilişim derslerine rastlanılmış olsa da siber güvenlik için yapay zekâ, siber güvenlik için veri madenciliği gibi derslere rastlanmamıştır. Fen bilimleri alanında, dijital dönüşüm ile siber güvenlik bağı kurulmuşken, sosyal bilimlerde bankacılıkta bu bağ kurulmamıştır. En azından 2 üniversitede (Akdeniz Üniversitesi ve Süleyman Demirel Üniversitesi) yapay zekâ ile finans arasında bir bağın kurulduğu derse (finansla yapay zekâ uygulaması gibi) rastlanmıştır. Ayrıca bankacılık müfredatlarında siber güvenliğin teknik boyutu (bilgisayar, internet, ağlar, algoritmalar, sızma testi, şifreleme gibi) sınırlı düzeyde olmakla birlikte muhasebe müfredatından daha kapsamlı ele alınmıştır.

Sonuç

Türkiye’de siber güvenlik farkındalığını artırmak için 124 üniversite, hem konunun muhataplarını bir araya getirmiş hem de siber güvenlik konusunu tüm yönleriyle (teknik-yasal-etik-eğitim-vatan-savaş) ele alarak muazzam faaliyetler gerçekleştirmiştir. Ancak bu faaliyetler süreklilik arz etmemiştir. Siber güvenlik farkındalığının her daim canlı tutulması için bu faaliyetlerin belirli aralıklarla yapılması gerektiği düşünülmektedir.

Siber güvenlik farkındalığı olmayan ya da olsa bile kurallara dikkat etmeyen kullanıcılar, kurumsal kimliğin daha büyük siber riskler altında kalmasına neden olmaktadır. Ülkemizdeki üniversitelerden 11’nin sahte sitesi yapıldığı ve üniversitelerin kurumsal kimliğine yönelik siber tehditlerin varlığı tespit edilmiştir. Özellikle kötü niyetli kişilerin hedefinde vakıf üniversitelerinin olduğu belirlenmiştir. ISO 27001 belgeli üniversitelerin sahte sitelerinin yapılması, kurumsal kimliğe yöneltilen tehdidin büyüklüğünü göstermektedir. Üniversiteler kurumsal kimliklerine yöneltilen tehditler için önlemler almalıdır ancak kullanıcılarının tehditler karşısındaki bilincini artırmak için de internet sitelerinde pop-up’lar yayınlamalıdır.

“Siber güvenlik” programları, siber güvenliğin teknik, dijital dönüşüm ve hukuki yönleri dikkate alınarak oluşturulmuştur. Dijitalleşme ile hayatımıza giren konuların özellikle siber güvenlikle bağı kurulmuştur. Hukuki yönü ise ulusal ve uluslararası düzenlemeleri kapsayacak şekilde ve derinliktedir. Siber güvenlik programları arasında 3 farklı düzeyde siber güvenlik eğitimi veren tek ve lider konumdaki üniversite İstanbul Ticaret Üniversitesi’dir.

Üniversiteler siber güvenlik konusunda muazzam faaliyetler gerçekleştirme kabiliyetlerini, muhasebe (15 program) ve bankacılık (43 program) ders müfredatlarını oluştururken yeterince gösterememiştir. Muhasebe programlarının 6’sında ve bankacılık programlarının 18’inde siber güvenlik eğitimine rastlanmamıştır. Bu durum, en az bir başarılı siber atak yaşayan % 95,7 ile birinci sırada yer alan finans sektörüne ilgili üniversitelerden mezun edilen öğrencilerin hangi donanımla mezun edildiği sorunsalı ortaya çıkmaktadır. 58 programında sadece 3’ünde “siber güvenlik” isimli derse rastlanmıştır. Ancak seçmeli ders olmasından dolayı, dersin aktif bir şekilde verilip verilmediği bilinmemektedir. “Siber hukuk” isimli derse ise hiç rastlanmamıştır. İlişkili içerik taşıyanlarda ise konuya yüzeysel yaklaşıldığı belirlenmiştir. Ayrıca siber güvenliğin teknik boyutu (fen bilimlerindekilerin derinliğinde ve çeşitliliğinde olmasa da) muhasebe ve bankacılık müfredatlarında sınırlı düzeyde ele alınmıştır.

Bankacılık müfredatları teknik boyutuyla, muhasebe müfredatlarından daha fazla derse sahiptir. “Siber güvenlik” programlarındaki gibi konunun savaş-güvenlik boyutunu ele alan bir derse de rastlanmamıştır.

Bu tespitler, Türkiye’yi siber saldırılar konusunda birinci sırada tutan nedenleri destekler niteliktedir. Muhasebe ve bankacılık programlarında siber güvenlik eğitimi vardır ama yeterli düzeyde değildir. Siber güvenlik eğitiminin yetersizliği, İstanbul Ticaret Üniversitesi’nin Çalıştay Raporu (2020:6) ile benzerlik taşımaktadır. Siber güvenlik tüm yönleri düşünülerek, dijital çağın ihtiyaçlarını karşılayacak şekilde müfredatlarda yerini almalıdır. Hukuk boyutu fen bilimlerindeki gibi zengin içerikli olmalı ve mümkünse ayrı bir ders olarak verilmelidir. Örneğin Birleşik Arap Emirlikleri, bir taraftan siber güvenlik için her yıl büyük altyapı yatırımları yaparken, diğer yandan siber güvenlik tehditlerine karşı hemen uyum sağlayabilecek etkili eğitim stratejileri belirlemiştir. Eğitim kurumlarının müfredatlarını artan siber tehdit türüne göre güncelleyerek, gerçek zamanlı tehdit yönetimi gerçekleştirebilmiş ve hafifletme stratejilerini uygulayabilmiştir. Tehditler karşısında eğitim müfredatlarını güncelleme kabiliyeti (hızı) ile siber güvenlik programlarına hukuki ve etik eğitimleri de entegre etmesi onu, Güney Kore ve Singapur karşısında benzersiz kılmıştır (İsmail, Madathil, Alalawi, Alrabace, Al Bataineh, Melhem & Mouheb, 2024:2). Mevcut müfredatların yenilenmesi zor ve zaman alan işlerdir. Siber güvenlik müfredatının geliştirilmesi amacıyla, Avrupa Siber Güvenlik Becerileri Çerçevesi⁸ni esas alan yapay zekâ destekli yenilikçi bir haritalama metodolojisi geliştirilmiş ve Çekya’daki bir üniversitenin müfredatına bu metodoloji uygulanmıştır. Söz konusu çerçevenin mevcut müfredatlara sorunsuz bir şekilde entegre edilebildiği ve dinamik sektör ihtiyaçları ile değişen trendlere etkili bir şekilde uyum sağlayabileceği belirlenmiştir (Dzurenda, Ricci, Sikora, Stejskal, Lendak & Adao, 2024). Ülkemizde kurulması planlanan Siber Güvenlik Başkanlığı ile Siber Güvenlik Becerileri Çerçeveleri yayınlanabilir ve Çekya’da uygulanan yapay zekâ destekli metodolojiden faydalanılarak ders müfredatları ihtiyaçlara cevap verebilen dinamik bir yapıya kavuşturulabilir. ABD’de AACSB⁹ akreditasyonuna sahip işletme okullarında verilen siber güvenlik programları (lisans) incelendiğinde en yaygın derslerin “siber güvenlik temelleri”, “uygulama geliştirme ve programlama” ve “BT altyapısı” olduğu belirlenmiştir (Yang, 2024:313). Ülkemizde muhasebe ile bankacılık müfredatlarında da siber güvenlik adında ayrı bir ders olmalı ve eğitim “Beyaz Şapkalı Hacker” donanımıyla verilmelidir. Üniversitelerin mühendislik bölümünden eğitim desteği alınabilir. Ayrı ders açılmıyorsa mevcut derslerin (temel bilgisayar kullanımı, dijital okuryazarlık gibi) içeriği siber güvenlikle zenginleştirilmez. Çünkü dijital okuryazarlık, gençlerin dijital ortamları bilinçli ve sorumlu kullanabilme becerisi üzerinde kritik bir etkiye sahiptir ve Kanada’da dijital okuryazarlık programları üzerine bir çalışma gerçekleştirilmiştir. Bu çalışmada, söz konusu programların gençleri dijital çağa daha iyi hazırladığı ve aynı zamanda teknoloji kullanımına bağlı potansiyel riskleri en aza indirmeye katkı sağladığı tespit edilmiştir (Buchan, Bhawra & Katapally, 2024). Böylelikle Türkiye’de muhasebe ve bankacılık müfredatlarındaki siber güvenlik eğitimine yönelik öneriler, çeşitli ülke uygulamalarıyla desteklenmiştir. Gelecekteki çalışmalar için farklı ülkelerin üniversitelerinde siber güvenlik farkındalığının oluşturulmasında hangi faaliyetlerin gerçekleştirildiği ve bunun eğitim müfredatındaki durumu araştırılabilir. Bu çalışma muhasebe ve bankacılık gibi spesifik bir alanda gerçekleştirilmiştir. Daha genel bir alan olan işletme bölümleri kapsamında, siber güvenlik eğitiminin durumu Türkiye ve dünyada öne çıkan üniversiteler açısından araştırılabilir ve karşılaştırmalı bir çalışma yapılabilir.

Çıkar Çatışması Beyanı

Yazar, bu makalenin araştırma, yazarlık ve/veya yayın süreci ile ilgili herhangi bir potansiyel çıkar çatışması olmadığını beyan eder.

Mali Destek

Yazar bu makalenin araştırılması, yazılması ve/veya yayınlanması için herhangi bir mali destek almamıştır.

Yayın Etiği Beyanı

Çalışmada etik dışı bir husus bulunmadığını, araştırma ve yayın etiğine özenle uyulduğunu beyan ederim.

⁸ Bu çerçeveler Avrupa Birliği Siber Güvenlik Ajansı (European Union Agency for Cybersecurity-ENISA) tarafından yayımlanmaktadır.

⁹ AACSB: Association to Advanced Collegiate Schools of Business-İşletme alanında eğitim veren fakültelerin en önemli küresel akreditasyon kurumu

Yazar Katkı Oranı

Çalışmanın tamamı tek bir yazar tarafından yürütülmüş ve raporlanmıştır.

Etik Kurul İzni

Bu çalışmanın etik kurul izni gerektirmeyen çalışmalardan biri olduğunu sorumlu yazar olarak beyan ederim.

Kaynakça

- Aksoğan, M., Bayer, H., Gülada, M.O., & Çelik, E. (2018). İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği. *Kesit Akademi Dergisi*, (13), 271-288. <https://dergipark.org.tr/tr/pub/kesitakademi/issue/59829/864303>
- Avcı, Ü., & Oruç, O. (2020). Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışları ve Bilgi Güvenliği Farkındalıklarının İncelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 21(1), 284-303. <https://doi.org/10.17679/inuefd.526390>
- Baz, F.Ç., & Uludağ, K. (2023). Siber Güvenlik Konusunda Bilgi İşlem Yönetici ve Çalışanlarının Farkındalıkları. *Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 6(Ek Sayı), 402-414. <https://doi.org/10.47495/okufbed.1233526>
- Bilecik Şeyh Edebali Üniversitesi (2024). *Temel Bilgi Teknolojisi Kullanımı*. <https://ebs.bilecik.edu.tr/pdf/dersbilgetir/396478> (Erişim Tarihi: 18.08.2024)
- Bilgi Üniversitesi. *Bilgi, Bilgi Konusundaki Yetkinliğini Uluslararası Düzeyde Tescilledi*. <https://www.bilgi.edu.tr/tr/haber/10799/bilgi-bilgi-guvenligi-konusundaki-yetkinligini-uluslararasi-duzeyde-tescilledi/> (Erişim Tarihi: 10.08.2024).
- Bir zincir ancak en zayıf halkası kadar kuvvetlidir. <https://gelisim.edu.tr/tr/gelisim-haber-siber-saldirilarda-en-zayif-halka-sirket-kullanilari#:~:text=Son%20boyut%20olan%20ve%20genellikle,insan%20fakt%C3%B6r%C3%BC%20olarak%20nitelendirilen%20kullan%C4%B1c%C4%B1lard%C4%B1r.> (Erişim Tarihi: 03.08.2024).
- Bu açıklamalar hangi teori kapsamında değerlendirilmelidir? <https://chatgpt.com/c/67c7897c-a3a4-8010-84d9-e72933cb671b>(Erişim Tarihi: 05.03.2025).
- Buchan, M.C., Bhawra, J., & Katapally, T.R. (2024). Navigating the digital world: development of an evidence-based digital literacy program and assessment tool for youth, *Smart Learning Environments*, 11(1). 10.1186/s40561-024-00293-x (Erişim Tarihi: 05.03.2025).
- CyberEdge Group (2023). *2023 Cyberthreat Defence Repoert North America, Europe, Asia Pasific, Latin America, Middle East, Africa*. <https://cyberedgegroup.com/wp-content/uploads/2023/04/CyberEdge-2023-CDR-Report-v1.0.pdf> (Erişim Tarihi: 19.08.2024).

- Cybersecurity Ventures (2023). 2023 Official Cybercrime Report. <https://www.esentire.com/resources/library/2023-official-cybercrime-report> (Eriřim Tarihi: 19.08.2024).
- Çakır, H., & Tařer, M. (2023). Türkiye’de Yapılan Siber Güvenlik Faaliyetlerinin ve Eđitim Çalıřmalarının Deđerlendirilmesi. *Gaři Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, 11(2), 347-366. <https://doi.org/10.29109/gujsc.1165131>
- Dzurenda, P., Ricci, S., Sikora, M., Stejskal, M., Lendak, I., & Adao, P. (2024, July 30-August 2). *Enhancing Cybersecurity Curriculum Development: AI-Driven Mapping and Optimization Techniques*, 19th International Conference on Availability, Reliability and Security, ARES 2024, Vienna, ACM International Conference Proceeding Series, Doi: 10.1145/3664476.3670467.
- Erdal, N., Filiz, M., & Budak, O. (2023). Kiřilik Özelliklerinin Siber Güvenlik Algısı Üzerine Etkisi: Z Kuřađı Örneđi. *Sinop Üniversitesi Sosyal Bilimler Dergisi*, 7(1), 643-670. <https://doi.org/10.30561/sinopusd.1256325>
- Erođlu Yalın, B., & řahin Bařfırıcı, Ç. (2018). Cybersecurity perceptions of university student in Turkey. *Karadeniz Teknik Üniversitesi İletişim Fakóltesi Elektronik Dergisi*, 5(16), 2-14. <https://dergipark.org.tr/en/download/article-file/824317>
- Garanti BBVA. (2024). 2024’te Siber Suçların Dünyaya Maliyeti Ne Kadar Olacak?. <https://www.garantibbva.com.tr/blog/siber-suclarin-dunyaya-maliyeti-ne-kadar-olacak> (Eriřim Tarihi: 10.08.2024).
- Gündüzalp, C. (2021). Üniversite Çalışanlarının Dijital Veri ve Kiřisel Siber Güvenlik Farkındalıkları (Bilgi İşlem Daire Başkanlıkları Örneđi). *Journal of Computer and Education Research*, 9(18), 598-625. <https://doi.org/10.18009/jcer.907022>
- Ismail, M., Madathil, N.T., Alalawi, M., Alrabae, S., Al Bataineh, M., Melhem, S., & Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey, *Computers in Human Behavior Reports*, 16. <https://doi.org/10.1016/j.chbr.2024.100501>.
- ISO 27001 Bilgi Güvenliđi Yönetim Sistemi, <https://belgelendirme.ctr.com.tr/iso-27001.html> (Eriřim Tarihi: 10.08.2024).
- ISO 27001:2022. <https://www.iso.org/standard/27001> (Eriřim Tarihi:10.08.2024).
- İstanbul Ticaret Üniversitesi. (2020). *Üniversitelerde Sunulan “Adli Biliřim ve Siber Güvenlik” Eđitim Programlarına Yönelik Mevcut Durum ve İhtiyaç Analizi Çalıştay Raporu*. https://ticaret.edu.tr/uploads/etkinlik/5881/Rapor_Adli%C5%9Fim%C5%9Fim%20ve%20Siber%20G%C3%BCvenlik%20%C3%87al%C4%B1%C5%9Ftay%C4%B1.pdf (Eriřim Tarihi: 03.08.2024).

- Karacı, A., Akyüz, H.İ., & Bilgici, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi. *Kastamonu Eğitim Dergisi*, 25(6), 2079-2094. <https://doi.org/10.24106/kefdergi.351517>
- Karakaya, A., & Yetgin, M.A. (2020). Karabük Üniversitesi Çalışanlarına Yönelik Kişisel Siber Güvenlik Üzerine Araştırma. *Kabramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi*, 10(2), 157-172. <https://doi.org/10.47147/ksuiibf.816171>
- Kırıkkale Üniversitesi .(2023). *Üniversitemizde Siber Alem ve Siber Güvenlik Konulu Panel Düzenlendi.* <https://kku.edu.tr/Anasayfa/Haber/Index/3172> (Erişim Tarihi:10.08.2024).
- NCSI- National Cyber Security Index. (2016-2023) <https://ncsi.ega.ee/ncsi-index/?type=c&archive=1>(Erişim Tarihi: 10.12.2024).
- Önaçan, M. B. K., & Atan, H. (2016). Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği. *Trakya Üniversitesi Mühendislik Bilimleri Dergisi*, 17(1), 13-21. <https://dergipark.org.tr/tr/pub/tujes/issue/21551/370293>
- Para Dergisi. (2024). *En çok siber saldırıya maruz kalan ülke: Türkiye.* <https://www.paradergi.com.tr/teknoloji/2024/03/15/en-cok-siber-saldiriya-maruz-kalan-ulke-turkiye> (Erişim Tarihi: 10.08.2024).
- Pop Up Nedir? <https://www.userspots.com/sozluk/pop-up-nedir#:~:text=Pop%20Dup%2C%20internet%20kullan%C4%B1c%C4%B1lar%C4%B1n%C4%B1n%20web,%C3%B6n%C3%BCnde%20beliren%20k%C3%BC%C3%A7%C3%BCk%20a%C3%A7%C4%B1%C4%B1r%20pencerelerdir> (Erişim Tarihi: 5.01.2025).
- Prototip Kuramı, https://tr.wikipedia.org/wiki/Prototip_kuram%C4%B1(Erişim Tarihi: 04.03.2025).
- Psikolojide Prototipler: Tanım ve Örnekler (2024). <https://helpfulprofessor.com/prototypes-psychology/>(Erişim Tarihi: 05.03.2025).
- STM Mühendislik, Teknoloji, Danışmalık (2023). *Ekim-Aralık 2023 Siber Tehdit Durum Raporu.* <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ekim-aralik-2023> (Erişim Tarihi: 18.09.2024).
- STM Mühendislik, Teknoloji, Danışmalık (2024). *Temmuz-Eylül 2024 Siber Tehdit Durum Raporu.* <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-temmuz-eylul-2024> (Erişim Tarihi: 30.12.2024).
- Şimşek, T. (2024). Planlı davranış teorisi kapsamında A/B kişilik tipine göre siber güvenlik farkındalığı: Üniversite öğrencileri üzerine bir araştırma. *Manas Sosyal Araştırmalar Dergisi*, 13(3), 1066-1074. <https://doi.org/10.33206/mjss.1300491>

- Tokmak, M. (2023). Öğrencilerin Siber Güvenlik Farkındalık Düzeylerinin Makine Öğrenmesi Yöntemleri ile Belirlenmesi. *Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 28(2), 451-466. <https://doi.org/10.53433/yyufbed.1181694>
- Tuğal, İ., Almaz, C., & Sevi, M. (2021). Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri. *Journal of Information Technologies - Bilişim Teknolojileri Dergisi*, 14(3), 229-238. <https://doi.org/10.17671/gazibtd.754458>
- Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-turjman, F., & Mostarda, L. (2019). Cyber-security threats Detection in Internet of Things Using Deep Learning Approach. *IEEE Access*, 7, 124379-124389 doi:10.1109/ACCESS.2019.2937347. (Aktaran, Admass, W.S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2(10031), 1-9. <https://doi.org/10.1016/j.csa.2023.100031>)
- We Are Social 2023 Global ve Türkiye Raporu. (2023). <https://www.clicksus.com/we-are-social-2023-global-ve-turkiye-raporu> (Erişim Tarihi: 10.07.2024).
- Yang, S.C. (2024). A Curriculum Model of Cybersecurity Bachelor's Programs in AACSB-Accredited Business Schools in the US. *Journal of Information Systems Education*, 35(3), 313-324. Doi: 10.62273/FRJE3390.

EXTENDED SUMMARY

In today's world where digitalization encompasses everyone from 7 to 70, our way of life has changed and all kinds of work and communication are carried out in digital environments over networks. Although digitalization has accelerated and facilitated workflows, it has also brought cyber risks. The threat of cyber-attacks on data security has made cyber security important. The aim of this study is to determine the status of cyber security education in accounting and banking (undergraduate) education in the field of social sciences in Turkey.

The research consists of three parts. In the first part, cyber security competencies and cyber security operations of universities in Turkey; in the second part, programs opened under the name of "cyber security" and their curricula; and in the third part, the projection of cyber security in social sciences in terms of accounting and banking departments were investigated. The official websites of the universities were scanned by conducting an in-site search and the collected data were analyzed using the content analysis method.

The findings of the research are as follows:

- While 61 out of 208 universities in Turkey have IEC 27001 certification, only 5 out of 208 universities have IEC 27001:2022 certification. 2 universities are in the process of transition to this certificate.
- It was determined that 11 universities in Turkey have fake websites under the name of "paid sponsored advertisement". In addition, 4 of the 11 universities have IEC 27001 certification.
- Only 4 universities in Turkey have published cyber security awareness raising/warning texts on their official websites, alerting academic and administrative staff and students. However, in these texts, only one university has raised awareness about the places to apply in case of a cyber-attack.
- It was determined that 124 out of 208 universities and 63 out of 81 provinces in Turkey are making a tremendous effort in cyber security-related activities. The top three activities are "cyber security promotion and awareness activities", "cyber security and career opportunities" and "cyber homeland".
- In Turkey, 22 out of 208 universities have opened a cyber security program: 5 associate, 1 bachelor, 19 master and 2 doctorate.
- Cyber security programs are mostly located in the field of engineering and natural sciences. The curricula in this field are designed not only in terms of technical infrastructure, but also in terms of cross-border cyber security (cyber warfare) and ethics-cyber law. The curricula also link digital transformation with cyber security. In other words, in addition to cloud computing courses, cyber security in cloud computing courses are also included in the curriculum. Cyber security-engineering and natural sciences curricula include ethics and cyber law courses. Cyber law courses have a rich content covering national and international regulations.
- Cyber security is available as an elective course only in the accounting and finance management department of Istanbul Aydın University. Başkent University has the richest curriculum with 7 courses on cyber security.
- Erzincan Binali Yıldırım University and İstanbul Nişantaşı University offer a separate course called "cyber security", even as an elective in banking departments. İstanbul Gelişim University has the richest curriculum with 9 courses on cyber security in banking programs.
- It was determined that there is no separate course called "cyber law" in accounting and finance management programs and banking programs. Cyber law, ethics, computing ethics have been covered only cursorily in a few of the courses on cyber security.

Universities in Turkey have made significant efforts to raise cyber security awareness. However, these activities are not continuous. It is thought that these activities should be carried out periodically to keep cyber security awareness alive at all times. Users who do not have cyber security awareness or who do not pay attention to the rules even if they do, cause the corporate identity to be under greater cyber risks. The fact that 4 universities with IEC 27001 certification have fake websites draw attention to the magnitude of the threat to corporate identity. Universities should take precautions against threats to their corporate identity, but at the same time, they should raise awareness of their users against threats by publishing pop-ups on their websites.

In Turkey, there are associate, bachelor's, master's and doctoral programs under the name of "cyber security" and their curricula have been created with a rich content taking into account the technical aspect, digital transformation aspect and legal aspect of cyber security.

Universities have not adequately demonstrated their ability to carry out tremendous activities in cyber security when creating their accounting and banking course curricula. While a course called "cyber security" was found in accounting and banking programs, albeit in limited numbers, the course called "cyber law" was not found. In addition, the technical and legal dimensions of cyber security have a limited content in accounting and banking curricula.

There is a cyber security education in accounting and banking programs in social sciences, but it is not a sufficient level. Cyber security should be included in the accounting and banking curriculum to meet the needs of the digital age, considering its technical, ethical, legal and homeland dimensions. The legal dimension should be as rich as in content the engineering and natural sciences curriculum and, if it is possible, should be given as a separate course. If it is not possible, the content of existing courses should be enriched with cyber security/cyber law.