T.C
SAHA İSTANBUL & TÜBİTAK TÜSSİDE
SAHA AKADEMİ MBA YÖNETİCİ GELİŞTİRME PROGRAMI

Ülkemizin Siber Güvenlik Yapılanması ve Siber Güvenlik Mevzuatının Avrupa Birliği ile Uyumu

MBA Proje
Murat YAZGAN

Danışman
Dr. Uğur TARÇIN
Ankara – 2025

ARAŞTIRMA PROJESİ UYGUNLUK FORMU

MBA: 2024-2025/71

1. SAHA İstanbul Yönetim Kurulu kararıyla, 2024-2025 eğitim döneminden itibaren SAHA AKADEMİ MBA katılımcılarına "Araştırma Projesi" hazırlama yükümlülüğü getirilmiştir. Bu uygulama; katılımcıların sektörel bilgi, stratejik düşünme ve akademik üretkenlik yetkinliklerini geliştirmeyi hedeflerken, savunma sanayii ekosistemine bilimsel katkıyı artırmayı amaçlamaktadır. Bu girişim, Türk savunma sanayii ekosisteminde bilimsel katkıyı artırmaya yönelik önemli bir adımdır.

2. SAHA İstanbul-SAHA AKADEMİ tarafından yayımlanan bu çalışma, ilgili yazar tarafından özgün biçimde hazırlanmış ve beyan edilmiştir. Çalışmada yer alan görüşler yazara ait olup, SAHA İstanbul'un kurumsal görüşünü yansıtmamaktadır. İçerikte sunulan bilgi, yorum ve sonuçların doğruluğu sorumlu yazara aittir. SAHA AKADEMİ; benzerlik oran tespitini yapmıştır.

3. Bu çalışma, [Murat YAZGAN] tarafından hazırlanmıştır. Araştırma Projesi danışman tarafından değerlendirilmiş ve sunumu [10 Haziran 2025] tarihinde yeterli görülerek kabul edilmiştir.

<u>Araştırma Projesi Sunum Jüri Üyeleri</u>

Başkan	Dr. Uğur Tarçın (*SAHA AKADEMİ Öğr.Görevlisi)*	*e-imzalıdır*
Üye	İlker Özkan (*Genel Sekreter Yrdc*)	*e-imzalıdır*
Üye	Pınar Erguvan Kaya (*SAHA İstanbul Kurumsal İlişkiler Müdürü)*	*e-imzalıdır*

(Formun aslı, imzalı olarak ilgili dosyada muhafaza edilmektedir.)

İçindekiler

ÜLKEMİZİN SİBER GÜVENLİK YAPILANMASI VE SİBER GÜVENLİK MEVZUATININ AVRUPA BİRLİĞİ İLE UYUMU (PROJE)

Murat YAZGAN

Sanayi ve Teknoloji Bakanlığı
murat.yazgan@outlook.com

ÖZET

Dijitalleşmenin hızlanmasıyla siber güvenlik stratejik bir öneme ulaşmıştır. Yapay zekâ, blok zincir ve bulut bilişim gibi yeni teknolojilerin yaygınlaşması tehditleri karmaşıklaştırırken güvenlik önlemlerini de geliştirmiştir. Ülkeler hibrit savaşlara yönelerek siber saldırıları stratejik bir araç olarak kullanmaktadır. Ülkemizde Siber Güvenlik Başkanlığı kurulmuş ve siber güvenlik çatı mevzuat çalışmaları son aşamaya gelmiştir. Sonraki aşamada Avrupa Birliği mevzuatına uyum, yerli üreticilerin desteklenmesi, test laboratuvarlarının kurulması ve siber güvenlik sertifikasyon süreçlerinin geliştirilmesi kritik öneme sahiptir. Bu çalışmalar, Türkiye'nin siber güvenlik alanında küresel rekabet gücünü artıracaktır.

1. Siber Güvenlik Yapılanması

Dijitalleşmenin hız kazanması, bilginin, gizliliğin ve sistemlerin korunmasına olan ihtiyacı da artırmaktadır. Bireylerin ve kurumların dijital varlıklarını koruma gereksinimi, siber güvenlik politikalarına ve teknolojik yatırımlara stratejik bir boyut kazandırmıştır. Yapay zekâ, blok zincir, büyük veri ve bulut bilişim gibi teknolojilerin yaygın kullanımı, siber tehditlerin daha karmaşık hale gelmesine neden olurken, aynı zamanda güvenlik önlemlerinin gelişmesini de tetiklemiştir. Kritik altyapıların güvenliğinin sağlanması ve kamu kurumlarının dijital sistemlerinin korunması, günümüz siber güvenlik stratejilerinin temel unsurları arasındadır. Bu çerçevede, sürekli değişen tehdit ortamına uyum sağlayabilecek çevik ve dinamik çözümler üretmek, siber güvenliğin en önemli gereksinimlerinden biri olmuştur.

Dünyada, konvansiyonel savaşların yerini hibrit savaşlara bıraktığı görülmektedir. Devlet destekli siber saldırılarla karşı ülkenin kritik altyapıları, özellikle enerji şebekeleri ve iletişim

sistemleri hedef alınmaya başlanmıştır. Siber saldırıların devlet politikalarının bir aracı olarak kullanılmasındaki artış savaş ve barış halleri arasındaki sınırı belirsizleştirmiş, ülkeler direk askeri saldırılar yerine siber saldırıları; siyasi, ekonomik ve askeri hedeflere yönelik düşük maliyetli yüksek etkili bir strateji haline getirmiştir.

Dünyada tüm bu gelişmeler yaşanırken ülkemiz siber güvenlik yapılanmasında; siber savunma, kapasite geliştirme ve denetim üst faaliyetleri bağlamında birçok paydaşın yetki ve sorumluluğunun bulunduğu görülmektedir. Ayrıca çatı mevzuat eksikliği; standartların oluşturulması, yetki dağılımı ve denetim etkinliği açısından birtakım sorunlar oluşturmaktadır.

Ülkelerin siber güvenlik alanında ön plana çıkarak rol model olabilmesi, kapsamlı bir siber güvenlik çatı mevzuatın varlığı ve merkezi bir otoritenin etkin işleyişiyle doğrudan ilişkilidir. Çatı bir mevzuat, ulusal düzeyde siber güvenlik politikalarının tutarlılığını sağlamanın yanı sıra kamu kurumları, özel sektör ve bireyler için bağlayıcı standartlar sunmaktadır. Ayrıca, uluslararası iş birliği ve karşılıklı tanınabilirlik açısından temel bir çerçeve sağlayarak, ülkenin küresel siber güvenlik ekosistemindeki konumunu güçlendirmektedir. Bu mevzuatın etkili bir şekilde uygulanması, merkezi bir otoritenin varlığıyla mümkün hale gelmektedir. Çünkü, merkezi bir yapı, kaynakların verimli kullanımını, hızlı ve koordineli karar alma mekanizmalarını desteklemekte ve aynı zamanda, tehditlerin daha etkili tespit edilmesi, müdahale süreçlerinin uyum içinde yürütülmesi ve stratejik hedeflere odaklanılması için bir temel oluşturmaktadır.

2024 yılında Uluslararası Telekomünikasyon Birliği tarafından yayımlanan Küresel Siber Güvenlik Endeksi verilerine göre “Rol Model Ülke” kategorisi içerisinde yer alan 46 ülkenin siber güvenlik yapısı ve mevzuatı incelendiğinde; bu ülkelerin yaklaşık %90’ı, kapsamlı bir çatı mevzuata sahip olup kişisel verilerin korunması, siber suçların önlenmesi ve kritik altyapıların güvenliği gibi konularda net bir hukuki çerçeve sunmaktadır. Ancak ülkemiz, “Rol Model Ülke” kategorisinde yer almasına rağmen gerçek anlamda çatı mevzuat özelliği teşkil edecek kapsamlı bir siber güvenlik kanununa sahip değildir. Çatı mevzuat eksikliği; veri güvenliği, ekosistem iş birlikleri, mevzuat düzenlemeleri, teşvik ve destekleri yönlendirme, uluslararası iş birlikleri, makro politika oluşturma ve benzeri birçok açıdan koordinasyon sorunları oluşturmaktadır. Çatı

mevzuatın oluşturulması ülkemizin küresel endekslerde üst sıralara yükselmesine katkı sağlayacaktır.

Tüm bu hususlar; ülkemizde halen farklı yapılar altında sürdürülmeye çalışılan siber güvenlik yaklaşımının, yeniden yapılandırılması ihtiyacını ortaya koymuştur. Nitekim 07.01.2025 tarihli ve 177 sayılı Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi ile Cumhurbaşkanlığına bağlı, kamu tüzel kişiliğini haiz, Siber Güvenlik Başkanlığı kurulmuştur. Kuruma siber savunma, kapasite geliştirme, gözetim ve denetim alanında görev ve yetkiler tanımlanmıştır. Konuya ilişkin olarak Türkiye Büyük Millet Meclisi (TBMM) Milli Savunma Komisyonuna, 2/2860 Esas numaralı Siber Güvenlik Kanunu teklifi sunulmuş olup Komisyon görüşmeleri tamamlanmıştır. Kanun teklifi ; 2025 yılı Mart ayı içerisinde TBMM Genel Kurulunda görüşülerek yasalaşmıştır.

Bu minvalde, siber güvenlik alanında merkezi yönetim mekanizması kurulmuş siber güvenlik yönetişimi çatı mevzuatı taslağı oluşturulmuştur. Ülkemize siber güvenlik alanında eşik atlatacak bu gelişmeye ek olarak yapılmasında fayda mülahaza edilen birtakım hususlar da bulunmaktadır. Siber güvenlik alanındaki düzenlemeleri, teşvik mekanizmaları, kurumları ve sivil toplum kuruluşları, ulusal stratejileri, uluslararası iş birlikleri ve potansiyel insan kaynağı ülkemizin güçlü yönleri olarak ön plana çıkmaktadır. Küresel düzeyde faaliyet gösteren firma sayısının azlığı, gözetim ve denetim alanındaki eksiklikler, eğitim ve öğretim müfredatı ise zayıf yanlar olarak görülmektedir. Kamu alımlarının kaldıraç etkisi olarak kullanılabilmesi, genç ve potansiyeli yüksek nüfusu fırsat şeklinde değerlendirilebilmektedir. Siber güvenlik ürün ve hizmetlerinde dışa bağımlılık, makro anlamda siber güvenlik alanının henüz yönetilememesi, bireylerin siber güvenlik farkındalığının yeterli seviyede olmaması ise tehditler olarak sıralanabilir.

Netice itibarıyla, ülkemizin siber güvenlik alanında attığı stratejik adımlar, merkezi yönetim mekanizmasının kurulması ve çatı mevzuat taslağının oluşturulmasıyla önemli bir eşiğe ulaşmıştır. Ancak, küresel ölçekte rekabetçi bir siber güvenlik ekosistemi oluşturmak için mevcut güçlü yönlerin daha da geliştirilmesi, zayıf yanların giderilmesi ve uluslararası iş birliklerinin güçlendirilmesi gerekmektedir. Eğitim programlarının geliştirilmesinden teknoloji üretimine,

mevzuat hazırlıklarından farkındalık çalışmalarına kadar bütüncül bir yaklaşım benimsenerek siber güvenlik alanında sürdürülebilir ve yenilikçi politikalar hayata geçirilmelidir. Böylece, ülkemiz hem ulusal düzeyde siber tehditlere karşı daha dirençli hale gelecek hem de küresel siber güvenlik ekosisteminde daha etkin bir konuma yükselecektir.

Çatı mevzuatın yasalaşması ve Siber Güvenlik Başkanlığı teşkilatlanmasını tamamlamasını müteakip özellikle siber güvenlik ürün ve hizmetlerin ticaretine odaklanılması yerinde olacaktır. Avrupa Birliği (AB) Komisyonu tarafından yayımlanmış olan 2022/30 sayılı delegated act ile Cyber Resilience Act (CRA) sırasıyla IoT ürünler ve dijital unsur içeren tüm ürünlerin piyasaya arz koşullarını düzenlemektedir. Bu kapsamda öncelikle Gümrük Birliği ve AB mevzuatından bahsetmek gerekmektedir.

2. Gümrük Birliği

"Teknolojiye sahip olan standarda, standarda sahip olan pazara hâkim olur." Pazara hâkim olan refah içinde yaşarken diğerleri küçülmeye mahkûm olur.

Ülkemiz ile AB arasında gerçekleştirilen müzakerelerin ardından 1/95 sayılı Ortaklık Konseyi Kararı ile yürürlüğe giren Gümrük Birliğinin uygulanması ile birlikte 1996 yılından bugüne sanayi ürünleri için gümrük vergileri, eş etkili vergiler ve miktar kısıtlamaları kaldırılarak bu pazarda malların serbest dolaşımında kolaylıklar sağlanmıştır. Konuya ilişkin olarak, ticarette teknik engellerin kaldırılması amacıyla Avrupa Birliği mevzuatına uyum yükümlülüğümüz ortaya çıkmıştır. Son 10 yıldır ülkemiz, ihracatının yüzde 50'den fazlasını Avrupa ülkelerine ve bunun da büyük kısmını AB üyesi ülkelere gerçekleştirmektedir. Bu bağlamda ülkemizin AB mevzuatını yakından takip etmesi, bu konuya proaktif yaklaşım sergilemesi önem arz etmektedir.

2.1 Siber Güvenlik Hizmet Mevzuatı

AB'de siber güvenlik hizmetlerine ilişkin ilk mevzuat 10 Mayıs 2018 yılında zorunlu uygulamaya giren NIS 1.0 (2016/1148) direktifidir. Bu direktif; enerji, sağlık, ulaştırma ve finans gibi kritik sektörlerde faaliyet gösteren işletmelere, siber tehditlere karşı daha yüksek düzeyde

güvenlik önlemleri alma ve olayları raporlama yükümlülüğü getirmiştir. Ayrıca, üye devletler arasında iş birliğini güçlendirmek amacıyla bir ulusal yetkili otorite ve bir bilgisayar güvenliği olay müdahale ekibi (CSIRT) oluşturulmasını zorunlu kılmıştır. Üye devletlere ulusal mevzuata aktarmaları için 17 Ekim 2024 tarihine kadar süre verilen NIS 2.0 (2022/2555), NIS 1.0 direktifini yürürlükten kaldırmıştır. Bu yeni direktif, kapsamını genişleterek daha fazla sektör ve kuruluşu içine alırken, siber risk yönetimi ve olay raporlama yükümlülüklerini daha net ve katı hale getirmektedir. Ayrıca, cezai yaptırımlar ve AB üye ülkeleri arasında daha güçlü iş birliği mekanizmaları getirerek, birlik genelinde daha yüksek bir siber güvenlik standardı oluşturmayı amaçlamaktadır.

2.2 Siber Güvenlik Ürün Mevzuatı

AB'de ürünlere ilişkin ilk siber güvenlik mevzuatı 1 Ağustos 2025 yılında uygulamaya girecek olan RED direktifine (RED-2014/53/EU) bağlı Delegated Act'tir (2022/30). Bu kapsamda, RED direktifine ağ güvenliği, kişisel verilerin güvenliği ve dolandırıcılığa karşı güvenliğin sağlanmasıyla ilgili 3 madde eklenmiştir.

AB siber güvenlik ürün güvenliğinin kapsamlı düzenlemesi ise Cyber Resilience Act'tir (CRA). CRA, 20 Kasım 2024 tarihinde Avrupa Birliği Resmî Gazetesi OJEU'da yayımlanmıştır. Tüm bileşenleri ile uygulanması 11 Aralık 2027'de, raporlama yükümlülükleri ise 11 Eylül 2026'da başlayacaktır.

Robot süpürgeler, işletim sistemleri, IoT ürünleri, güvenlik duvarları, mikroişlemciler, PLC ve SCADA sistemleri, endüstriyel otomasyon ve kontrol sistemleri gibi ürünler de dahil olmak üzere dijital unsur barındıran tüm yazılım ve donanım ürünleri CRA kapsamı dahilinde bulunmaktadır. CRA, yazılım ve donanım dâhil dijital unsur barındıran ürünlerin tasarımı, geliştirilmesi, üretimi ve piyasaya arz edilebilmeleri için karşılamaları gereken zorunlu siber güvenlik gereksinimlerini belirlemektedir. CRA'nın temel amacı donanım ve yazılım ürünlerinin piyasaya daha az güvenlik açığıyla sunulmasını sağlamaktır.

2.3 Siber Güvenlik Sertifikasyon Şemaları

AB'de siber güvenlik sertifikasyon şemalarına esas teşkil eden düzenleme 28 Haziran 2021 tarihinde uygulamaya giren Cyber Security Act'tir (CSA-2019/881). CSA'nın temelde iki amacı vardır; bunlardan ilki ENISA'ya (AB Ağ ve Bilgi Güvenliği Ajansı) kalıcı bir yetki vermek diğeri ise AB siber güvenlik sertifikasyon şemasını oluşturmaktır. CSA altında EUCC (EU Common Criteria), EUCS (EU Cloud Services) ve EU5G olmak üzere 3 tür sertifikasyon şeması öngörülmüştür. Sertifikasyon şemasının temel amacı ürünlerin ya da hizmetlerin belirli güvenlik seviyesine uygun olduğunu belgelemektir. Sertifikasyon şemalarının şu an için tamamıyla gönüllü bir şekilde yürütülmesi planlansa da önümüzdeki dönemde özellikle kamu kurumları ve kritik altyapılarda zorunlu tutulması beklenmektedir. Ayrıca, ürünlerini sertifikasyon şemasına tabi tutan üreticilerin tüketici güvenliği açısından piyasada rekabetçi konuma erişebileceği de unutulmamalıdır.

2.4 Standardizasyon

Siber güvenlik konusunda AB Komisyonunun AB'nin üç standardizasyon kuruluşundan biri olan ETSI (Avrupa Telekomünikasyon Standartları Enstitüsü) yerine diğer iki kuruluş CEN (Avrupa Standartlar Komitesi) ve CENELEC (Avrupa Elektroteknik Standartlar Komitesi) ile çalışma prensibine kaydığı gözlenmiştir. 01.08.2025 tarihinde zorunlu uygulamaya girecek olan "2022/30 sayılı delegated act" için (2014/53/EU direktifinin siber güvenlik maddeleri) ETSI 303 645 (Tüketici IoT siber güvenliği) standardı bulunmasına rağmen CEN ve CENELEC'e harmonize standart hazırlama görevi vermesi ve CEN tarafından EN 18031 standardı kapsamında çalışma yapılması bu duruma örnek gösterilebilir.

Burada, CRA'nın zorunlu uygulamaya girmesi akabinde 2014/53/EU direktifinin siber güvenlik maddelerini de kapsayacağını ve dolayısıyla ilga edeceğini ifade etmek uygun olacaktır. Özellikle, CRA altında yer alacak harmonize standartlar için CEN-CLC/JTC 13'ün çalışmaya başlaması güzel bir örnektir.

Siber Güvenlik Başkanlığının standartların yayınlanma sürecini takip ederek yayını akabinde Türk Standardları Enstitüsü ile iş birliği içinde iç mevzuata kazandırma çalışmalarına öncülük etmesi önemlidir.

2.5 Onaylanmış Kuruluşlar

CRA kapsamındaki ürünler için üreticilerin bazı uygunluk değerlendirme prosedürleri işletmesi gerekmektedir. Bu 3 prosedür; iç kontrol prosedürü (modül A) veya AB tip inceleme prosedürü (modül B) ile birlikte iç üretim kontrolüne dayalı AB tipine uygunluğun sağlanması (modül C) veya tam kalite güvencesine dayalı uygunluk değerlendirme (modül H) olarak tanımlanmıştır.

Bilindiği üzere; modül B, modül C ve modül H üreticilerin onaylanmış kuruluş ile çalışmasını zorunlu kılan modüllerdir. CRA mevzuatı, ekinde sınıf I (koşullu olarak öngörmektedir) ve sınıf II olarak belirlenmiş dijital unsur içeren kritik ürünler için onaylanmış kuruluş ile çalışılması gerektiğini öngörmektedir.

Yerli onaylanmış kuruluş yerli üreticiler için kolaylık sağlamaktadır. Şöyle ki, yerli üreticinin yabancı onaylanmış kuruluş ile çalışması durumunda yerli üretici için yüksek maliyet oluşabilmektedir. Özellikle, ülke içerisinde yaşanabilecek kısıtlamalarda (pandemi gibi) yabancı onaylanmış kuruluşlar diğer ülkelerde hizmet sürekliliğini sağlamayabilmektedir. Bu da yabancı onaylanmış kuruluş ile çalışan üreticiyi zor durumda bırakarak üretimin aksamasına neden olabilmektedir. Diğer taraftan, belgelendirme faaliyetinin doğası gereği onaylanmış kuruluş ürün ve üretici üzerinde detaylı incelemeler ve sorgulamalar yapmaktadır. Yerli üreticinin yabancı onaylanmış kuruluşa mahkûm bırakılması ürününe ait önemli bilgilerin yurtdışına transferi anlamına gelmektedir.

CRA mevzuatı kapsamında yerli onaylanmış kuruluş atama sürecinin gecikmesi yerli üreticileri yabancı onaylanmış kuruluşlara mahkûm edecektir. Sonrasında yerli onaylanmış kuruluş atansa dahi yerli üretici, ek iş yükü gerektirecek olması ve operasyonlarını kaydırmak istememesinden kaynaklı olarak yerli onaylanmış kuruluşu tercih etmeyerek yabancı onaylanmış kuruluş ile çalışmaya devam edebilecektir. Bu anlamda, proaktif yaklaşım benimsenerek yerli onaylanmış kuruluş atama sürecinde gecikmeye mahal verilmeksizin işlem tesis edilmesi önem arz etmektedir.

Yerli onaylanmış kuruluşların yetkilendirilmesi akabinde yurtdışındaki üreticilere de hizmet vermesi adına cesaretlendirilmesi önem arz etmektedir. CRA mevzuatının uyumlaştırılması ve yardımcı mekanizmaların hazır hale getirilmesinde diğer ülkelere nazaran daha hızlı hareket edilmesi yerli atanacak onaylanmış kuruluşların hizmet ihracatının bir parçası olarak Avrupa pazarında söz sahibi olması açısından önemlidir.

2.6 Test Laboratuvarları

Dijitalleşme ve teknolojik gelişimi ile birlikte piyasaya arz edilen yazılım ve donanım ürünlerinde ciddi artış yaşanmaktadır. Ülkemizin Gümrük Birliği kapsamındaki taahhütleri ve ticaret hacmi hem üretilen ürünler hem de gümrüklere intikal etmiş ürünlerin siber güvenlik yönünden incelenmesini zorunlu kılmaktadır. Farklı uzmanlık alanlarını kapsayan, üreticilerin tasarım ve geliştirme aşamalarında destek alabileceği IoT cihazları, yazılım ürünleri ve diğer dijital ürünlerin test edileceği akredite laboratuvarlara ihtiyaç duyulmaktadır.

Türkiye'de yetkili test laboratuvarlarının kurulması, yerli ve yabancı yatırımcıları teşvik edecek, test hizmetlerinin yurtdışı yerine yurtiçinde yapılmasını sağlayarak döviz çıkışını önleyecek ve nitelikli istihdam yaratacaktır. Yeni test laboratuvarlarının kurulumu, yüksek maliyetler ve ileri teknik bilgi birikimi gerektirdiğinden devlet desteği kritik bir rol oynamaktadır. Laboratuvar yatırımlarını teşvik etmek amacıyla sağlanacak devlet teşvikleri hem ulusal güvenliğin güçlenmesi hem de yerli teknoloji üreticilerinin uluslararası pazarda rekabet edebilirliğinin artırılması açısından önem taşımaktadır. Test laboratuvarları ürünlerini test etmek isteyen ve geliştirmek isteyen üreticiler, ürünleri belgelendirmek isteyen onaylanmış kuruluşlar ve ürünlerin teknik mevzuata uygun olarak piyasaya arz edilip edilmediğini belirleyecek piyasa gözetimi ve denetimi otoriteleri için olmazsa olmaz bir altyapı olarak öne çıkmaktadır.

Siber Güvenlik Başkanlığı'nın test laboratuvarları konusunu önceliklendirerek kurulum ve geliştirme aşamalarına destek verilmesi gerektiği değerlendirilmektedir.

3. Türkiye Açısından Değerlendirme

Siber güvenlik sertifikasyon şemalarından EUCC "common criteria" temelinde ilerleyecektir. "Common criteria" ISO/IEC 15408 standardı kapsamında bilgi teknolojileri ürünlerinin güvenlik özelliklerini değerlendirmek ve sertifikalandırmak için çerçeve sunmaktadır.

Ülkemizde Sanayi ve Teknoloji Bakanlığı ilgili kuruluşu Türk Standardları Enstitüsü (TSE), 2003 yılında CCRA (Common Criteria Recognition Arrangement) anlaşmasını imzalayarak programa sertifika müşterisi rolünde üye olmuştur. Üyelik akabinde yapılan çalışmalar neticesinde 2010 yılında sertifika üreticisi konumuna yükselmiştir. Böylece ülkemiz; Amerika Birleşik Devletleri, Japonya, Almanya, Fransa, Kanada, Güney Kore gibi gelişmiş ülkelere benzer şekilde bu alanda sertifika üretebilen ülkelerden biri olmuştur. Günümüzde sertifika üretebilen 18 ülke, müşteri rolünde ise 13 ülke olmak üzere CCRA'ya taraf 31 ülke bulunmaktadır.

"Common criteria" kapsamında TSE tarafından ülkemizde akredite edilen 4 adet laboratuvar (Beam Teknoloji A.Ş., Certby Lab, STM ITSEF, TÜBİTAK BİLGEM OKTEM) bulunmaktadır. Hem yurtiçi hem de yurtdışı ihtiyaca cevap verebilecek bu laboratuvarların hem yazılım hem de donanım testleri yönünden kapasite artırımına gitmelerinin önem arz ettiği değerlendirilmektedir. TSE tarafından gerçekleştirilen bu faaliyetler ülkemizin EUCC'ye uyumu açısından birçok fırsatı barındırmaktadır. Kamu kurumları ve kritik altyapılarda kullanılacak ürünlere yönelik mekanizmanın benzer bir metodoloji ile devreye alınması hem siber dayanıklılık hem de kapasite geliştirme açısından ülkemize benzersiz faydalar sağlayacaktır. Üreticilerimizin bu sertifikasyonlara sahip olması küresel ölçekte ihracat kapasitemize doğrudan etki edecektir.

CRA, Sanayi ve Teknoloji Bakanlığı tarafından yakından takip edilmekte olup AB Komisyonu nezdinde iletişim kanalları kurulmuştur. İlgili kamu kurumlarına gerekli bilgiler sağlanmış olup sektörün bilinçlendirilmesine yönelik faaliyetler sürdürülmektedir. CRA kapsamında mevzuatın uyumlaştırılması, etki analizi, onaylanmış kuruluşlar ve test laboratuvarları kapsamında proaktif çalışmalar devam etmektedir. Siber güvenlik ekosistemi ile görüş alışverişinde bulunularak yürütülen bu çalışmalar neticesinde ülkemizin siber güvenlik altyapısının geliştirilmesi

hedeflenmektedir. CRA'nın üreticilerimiz ve ülkemiz ihracatı nezdinde oluşturabileceği tehditlerin bertaraf edilerek fırsata dönüştürülmesi kamu kurumları başta olmak üzere tüm ekosistemin katkıları ile mümkün hale gelebilecektir.

Diğer taraftan, Siber Güvenlik Başkanlığı'nın kurulmuş olması ve çatı mevzuat hazırlıklarının tamamlanmasın siber güvenlik alanındaki çalışmaların daha etkin ve verimli şekilde yürütülmesini mümkün kılacaktır.

4. Sonuç

Ülkemiz; TSE ve TÜBİTAK gibi kurumları, teknoparkta yer alan şirketleri, Ar-Ge merkezleri, sivil toplum kuruluşları ve teknoloji ekosisteminde yer alan diğer tüm aktörleri ile güçlü bir altyapıya ve beşerî sermayeye sahiptir. Bu potansiyelin, ortak akıl ve katılımcı yaklaşımla değerlendirilmesi, ülkemiz siber güvenlik ekosisteminin atılım yapmasını mümkün kılacaktır.

5. Kaynakça

Türkiye İstatistik Kurumu (2023). Ülke Gruplarına Göre İhracat. https://data.tuik.gov.tr/Kategori/GetKategori?p=dis-ticaret-104&dil=1, Erişim tarihi: 5 Mart 2025.

Common Criteria Portal (2024). Members of the CCRA. https://www.commoncriteriaportal.org/ccra/members/index.cfm. Erişim tarihi: 18 Kasım 2024

Common Criteria Portal (2025). Licensed Laboratories. https://www.commoncriteriaportal.org/labs/index.cfm. Erişim tarihi: 1 Mart 2025

Yazgan, M. (2023, Aralık). Anahtar. Avrupa Birliği Taslak Siber Dayanıklılık Yasası: Ülkemiz İçin Fırsatlar ve Tehditler. 420, 19-21.

Yazgan, M. (2025, Şubat). Cyber Spot. Avrupa Birliği Siber Güvenlik Düzenlemeleri: Ülkemiz Açısından Değerlendirme. 33, 6-8.

Yazgan, M. (2025, Şubat). Anahtar. Ülkemizin Siber Güvenlik Yapılanması ve Gelecek Perspektifi. 434, 9-10.