Türkiye'de Kritik Altyapı ve Siber Güvenlik

Uğur Özker

İçindekiler

YÖNETİCİ ÖZETİ 4

SİBER SALDIRI, GÜVENLİK & KRİTİK ALTYAPI KAVRAMLARI 5

Kritik Altyapı & Günümüzde Önemi 5

Geçmişten Günümüze Kritik Altyapıları Hedef Alan Etkili Siber Saldırılar 6

Yapay Zeka & Büyük Veri Destekli Teknolojilerin Gelişimi 9

DÜNYADA YAPILAN ÇEŞİTLİ ÇALIŞMALAR & DÜZENLEMELER 10

Avrupa Birliği Tarafından Gerçekleştirilen Çalışmalar 10

ABD Tarafından Gerçekleştirilen Çalışmalar 16

NATO 17

TÜRKİYE'DE MEVCUT DURUM VE YAPILAN ÇALIŞMALAR 20

Regülasyon ve Kamusal Düzenlemeler 20

İş Birlikleri & İlgili Kurumlar 21

DEĞERLENDİRME & ÖNERİLER 25

KÜNYE 32

Yazar: Uğur Özker 32

YÖNETİCİ ÖZETİ

Güçlü bir siber savunma, bir yanda kamu güvenliğinin, diğer yanda kritik altyapının tam bir dijital dönüşümden geçtiği günümüz dünyasında kritik bir yetenektir. Siber saldırı yöntemleri, uygulama maliyetlerinin düşük olması nedeniyle dünyadaki en büyük ve en hızlı büyüyen suç kategorilerinden biridir. Ayrıca kritik altyapılara uygulandığında verebileceği zararın büyüklüğü de siber saldırıları saldırganlar için çekici kılan bir başka nedendir.

Siber saldırıların sorumluları, çevrimiçi olarak çalınan finansal varlıklardan, veri ihlallerinden ve kritik altyapı operatörlerinin kesintiye uğraması nedeniyle sivil topluma verilen zarar ve kayıplardan doğrudan sorumludur. Mali kayıplar ve kritik altyapıların hasar görmesi her yıl milyarlarca ABD doları kayba neden oluyor ve bazı sektörlerde saldırı girişimleri her yıl iki ile üç kat artıyor.

Siber saldırıların bu kadar hızlı bir ivmeyle artmasının üç temel sebebi vardır. Birincisi, operasyonel teknoloji alanında iş süreçlerini içeren sanayii kuruluşlarının sinyalizasyon, sensör teknolojisine dayalı dijital dönüşümü ve nesnelerin interneti teknolojilerinin her geçen gün daha fazla kullanır hale gelmeleri ve otomasyon sistemlerinin tümüyle bu argümanlardan oluşmasıdır. Operasyonel teknolojinin parçası haline gelen bu alt sistemler üzerinde yaşanabilecek bir siber saldırı, fiziksel dünyada büyük etkiler yaratabilecek pek çok sonucu da beraberinde getirir.

Siber saldırıların artışındaki bir diğer sebep finansal sistemlerin her geçen gün biraz daha çevrimiçi hale gelmesidir. Finansal teknoloji, hayatımızı kolaylaştırdığı kadar riskli bir hale getiriyor. Özellikle bankalar gibi finans kuruluşları dijital dönüşümü gerçekleştirirken oldukça temkinli olmalıdır. Yaşanabilecek en ufak bir hata saniyeler içerisinde milyonlarca ABD doları kayıp ile sonuçlanabilmektedir. Öyle ki, bunun cazibesini gören siber saldırganlar tarafından SWIFT gibi global sistemler üzerinden devletlerin merkez bankaları bile sıklıkla hedef alınmaktadır.

Siber saldırıyı popüler kılan üçüncü ve son sebep ise kolaylığıdır. Ayrıca, saldırganların kimliğinin çoğunlukla anonim kalması da kolay olduğu kadar cazip kılan bir başka unsurdur. Bugün pek çok farklı tipte saldırı yöntemi hibrit olarak kullanılabiliyor ve genellikle hedef alınan mağdurların bilgi eksikliği ve hatalarından kaynaklanan nedenlerle kritik altyapı sistemlerini tamamen savunmasız ve açık hale getirebiliyor.

Tüm bu nedenleri bir araya getirdiğimizde siber casusluk çok tehlikeli ve yaygın. Dünyanın en büyük şirketleri ve kamu kurumları bile her yıl çevrimiçi sistemler aracılığıyla terabaytlarca fikri mülkiyet ve finansal varlıklarını kaybediyor. İsimsiz ve kötü niyetli saldırganlar elektrik şebekelerimizi, ulusal finansal sistemlerimizi, telekomünikasyon altyapılarımızı, sağlık kuruluşlarımızı ve hatta nükleer santrallerimizi tehdit ediyor. Sonuçta, kritik altyapılar siber saldırıların hedefi olduğunda ortaya çıkan tehdit, kamu sektörünün ötesinde tüm toplum için bir risk oluşturmaktadır.

Türkiye, jeopolitik konumu nedeniyle her gün sayısız siber saldırının hedefi olmaktadır. TANAP, Mavi Akım, Bakü-Ceyhan-Tiflis Boru Hattı gibi önemli enerji projeleri nedeniyle Türkiye, özellikle enerji alanında diğer ülkeler için de çok önemlidir. Ayrıca ülke, 51 farklı yerli ve yabancı uluslararası banka kuruluşu ile başta Orta Doğu – Afrika ve Avrupa bölgesi olmak üzere önemli bir uluslararası finansal hizmet sağlayıcısıdır. Tüm bunlara ek olarak, ülkenin Asya ve Avrupa kıtalarının bağlantı noktası olduğunu ve üç tarafının ticari denizlerle çevrili olduğunu düşündüğümüzde kritik altyapının tüm sektörlerinde ne kadar büyük bir tehlike ile karşı karşıya olduğunu rahatlıkla anlayabiliriz.

SİBER SALDIRI, GÜVENLİK & KRİTİK ALTYAPI KAVRAMLARI

Kritik Altyapı & Günümüzde Önemi

Siber güvenlik ve kritik altyapı, çağdaş güvenlik yapısı içinde tartışılması gereken en önemli konulardan biridir. Kritik altyapılara yönelik siber saldırıların arkasında birden çok neden var. ABD İç Güvenlik Bakanlığı'na göre kritik altyapı (CI), "ister fiziksel ister sanal olsun varlıklar, sistemler ve ağlardan" oluşur. "NATO'nun 2030 gündeminin ilk sıralarında da artan siber tehditler var".[1]

Dünya Ekonomik Forumu verilerine göre, 2001 ile 2018 yılları arasında ABD'deki İnternet Suçları Şikayet Merkezi'ne bildirilen şehirlerdeki kritik altyapıları hedef alan siber saldırıların neden olduğu mali kayıplar, 17,8 milyon ABD Dolardan 2,71 milyar ABD Dolara yükseldi.[2] Yıllara göre hızlı artışın nedeni online bağlantıların artması olmuştur. Erken aşamadaki virüsler, kurulum öncesi sektör virüsleriydi ve yalnızca virüs bulaşmış paylaşım bilgisayarlarının kullanıcıları tarafından kullanılan disketlerle sınırlandırılmış yerel bir bilgisayara bulaşabiliyordu. İnternet hizmeti daha yaygın hale geldikçe, disketlere yayılan virüslerin yerini yavaş yavaş e-postaların bir kısmına eklenen diğer virüsler aldı. Bu virüsler veri dosyalarına eklenecek şekilde tasarlanmıştır ve günümüzde birçok saldırı bu şekilde gerçekleştirilmeye devam etmektedir.

2021 yılı itibarıyla sadece ABD kuruluşlarında kritik altyapıların korunması için ayrılan bütçe bir önceki yıla göre 9 Milyar ABD Doları artarak 105,99 Milyar ABD Dolara ulaştı,[3] ve artışın yüksek bir ivme ile devam ederek 2027 yılında 154,59 Milyar ABD Doları ulaşması beklenmektedir.[4] Bu artışın temel sebebi ise COVID-19 pandemisinin uzaktan çalışma ile birlikte getirdiği güvenlik sorunları. Kritik altyapıdan sorumlu BT personeli ve diğer hizmet birimleri, giderek daha konforlu hale gelen konumdan bağımsız çalışma ortamına rağmen sistem ve hizmetlerin sorunsuz çalışmaya devam etmesini sağlamak için daha fazla önlem almak zorunda kaldı. Bu nedenle, altyapı operasyonlarının yetkili personel tarafından uzaktan güvenli bir şekilde izlenmesi ve yönetilmesi günümüzde her zamankinden daha kritik hale geldi.

Tüm bilgi teknolojileri endüstrisi ve özellikle ABD'deki paydaşlar için 2020'deki Solarwinds Orion Saldırısı, güvenli bağlantıya öncelik verme konusunda bir dönüm noktası oldu. Solarwinds'in SEC ile paylaştığı bilgilere göre bu saldırıda çoğunluğu sivil toplum kuruluşları ve kamu kurumları olmak üzere 18 bin Orion müşterisi aldıkları güncelleme ile sistemlerini saldırı altında buldu.[5] Daha da kritik olanı, bu kurumların Pentagon'u ve ABD hükümeti içindeki diğer birçok bakanlığı içermesiydi. Bu saldırı yoluyla yapılan izinsiz girişin ölçeği, zayıf bağlantılara sahip sistemlerin ne kadar savunmasız olabileceğini ve erişim sağlandıktan sonra tehdit edici aktörlerin ne kadar kolay aksiyon alabileceğini açıkça göstermektedir.

[1] NATO CCDOE, Cyber Threads & NATO 2030: Horizon Scanning & Analysis, https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf, 01.12.2020, Chapter 1
[2] World Economic Forum, Our Cities are Increasingly Vulnerable to heres How They Can Fight Back, https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/ , 30.09.2019
[3] ABI Research, Cybersecurity Spending for Critical Infrastructure to Surpass US$105 Billion in 2021 [website], https://www.abiresearch.com/press/cybersecurity-spending-critical-infrastructure-surpass-us105-billion-2021/ , (10 February 2021)
[4] Fortune Business Insights, Critical Infrastructure Protection Market, https://www.fortunebusinessinsights.com/critical-infrastructure-protection-cip-market-103339 , (01 July 2020)
[5] Business Insider, Solarwinds hack explained government agencies cyber security [website], https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 , (15 April 2021)

Saldırıların ardından birçok ülke sırasıyla siber güvenlik strateji planlarını açıklamaya başladı. Örneğin, 7 Şubat 2022 tarihinde yayınlanan İngiltere'nin Ulusal Siber Stratejisi 2022'ye göre[6], İngiltere'nin amacı, "Dünya'nın önde gelen siber gücü ve saldırılara dayanıklı demokratik bir ulus" olmaktır.[7] ABD tarafında, Başkan Joe Biden'ın Ulusal Siber Güvenliği İyileştirmeye Yönelik Eylem Planı, Federal Hükümetin özel sektör ve kamu sektörüyle işbirliğine odaklanıyor.[8] 2015 yılında, Fransa diğer ülkelere göre çok daha erken harekete geçerek 5 ana hedef üzerine kurulu bir eylem planı açıklamıştır. Bilgi sistemlerinin ve kritik altyapıların korunması, kişisel verilerin güvenliği, eğitim/farkındalık, uluslararası işbirlikleri ve işletmelerin bilgi teknolojileri ortamının güvenliği temel amaçları arasındadır.[9] Kritik altyapıların 5 ana hedefin başında yer alması, ulusların erken dönemlerden bu yana kritik altyapıların korunmasına verdikleri önemi ve önceliği açıkça göstermektedir. Aynı şekilde Türkiye Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) 29 Aralık 2020 tarihinde yayımlanmıştır.[10]

Geçmişten Günümüze Kritik Altyapıları Hedef Alan Etkili Siber Saldırılar

Ukrayna Güç Şebekesi Saldırısı - 2015
23 Aralık 2015 tarihinde, Ukrayna'da hizmet veren 3 farklı elektrik dağıtım şirketinin hizmet merkezlerine uzaktan izinsiz erişim sağlanarak 30 farklı trafo merkezinde devre kesici uygulandı ve bunun sonucunda başkent Kiev ile Ivano-Frisk bölgelerinde 230.000'den fazla abone saatlerce enerji hizmetinden mahrum kaldı.

Böylesine kapsamlı ve kamu hizmetlerini devre dışı bırakacak kadar planlı bir siber saldırının ilk aşamaları henüz 2015 baharında başlamıştır. Elektrik dağıtım şirketlerinden birinin beyaz yakalı bir çalışanı kendisine gelen bir e-postanın ekini açtığında farkında olmadan hedefli oltalama saldırısının kurbanı oldu ve kötü amaçlı bir yazılımın tetiklenerek, ofis dizüstü bilgisayarı sayesinde dağıtım şirketinin iç ağına yerleşmesini sağladı. Sistemlere sızmak için kullanılan BlackEnergy[11] kötü amaçlı yazılımı, 2014 yılından beri enerji kuruluşlarına sızmak için kullanılıyor.

Elektrik dağıtım şirketinin, biri BT ağı ile İnternet arasında, diğeri ise BT ve OT (endüstriyel) ağı arasında olmak üzere iki farklı ağ sistemi ve her ağ sisteminin üzerinde ayrı ayrı güvenlik duvarı bulunmaktaydı. Etkili bir saldırının yapılabilmesi için her iki güvenlik duvarını da aşarak iç ağa dahil olmak ve sonrasında OT ağı üzerinde yer alan trafo merkezlerine devre kesici komutlarını göndermek gerekiyordu. Sadece hedefli oltalama saldırısı ile bu gerçekleştirilemez, fakat ilk aşamada başarılı olan bu saldırı sayesinde bir sonraki aşama için gereken tüm bilgileri sistem katılımcılarının bilgisayarları bir süre izlenerek sağlanabilirdi.

Saldırının ikinci aşamasında birkaç ay boyunca, BlackEnergy kötü amaçlı yazılımı, kuruma özel verileri toplamak, adım adım tüm sunucu sistemlerine sızmak, güvenlik açıklarını tespit etmek ve trafoların

[6] HM Government, Government Cyber Security Strategy 2022 -2030, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf , (7 February 2022)
[7] HM Government, Government Cyber Security Strategy 2022 – 2030, p-8 Vision & Aim section 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf [web document], (7 February 2022)
[8] The White House, Executive Order on Improving the Nation's Cyber Security, Section 1, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, (12 May 2021)
[9] Premier Ministre, French National Digital Security Strategy [web document], https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf , (16 October 2015)
[10] Ulaştırma ve Altyapı Bakanlığı, Ulusal Siber Güvenlik Stratejisi Eylem Planı 2020 – 2023, http://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf [web document], (29 December 2020)
[11] State of New Jersey CCIC, ICS Malware Variants – BlackEnergy, https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/blackenergy [website], (10 August 2017)

kontrol edildiği endüstriyel otomasyon ağına girerek izleme faaliyetlerini gerçekleştirmek için uzaktan kontrol edildi. Gereken tüm bilgiler gelişmiş kalıcı tehdit (APT) ve keylogger ile toplandıktan sonra çalışanların bilgisayar başında olmadığı kısa bir süre içerisinde saldırı yapılacak sunuculara uzaktan bağlanarak malware yazılımları yüklenip sistem saldırı günü için hazır hale getirildi.

23 Aralık günü, saldırgan saldırının son ve üçüncü aşamasını başlatarak OT sunucularına uzaktan bağlandı ve devre kesicileri hızla kapatmaya başladı. Dağıtım şirketi operatörleri uzak bağlantıyı kesmek ve kapanan trafoları tekrar aktif hale getirmek için çabaladılar fakat ikinci aşamada keylogger ile operatörlerin şifresini ele geçiren saldırgan tüm şifreleri saldırı öncesinde değiştirerek, saldırı sırasında müdahale edilmesinin önüne geçmiş oldu. Tüm saldırı 10 dakika içerisinde gerçekleşti ve ayrıca saldırgan sunuculardaki diskleri silerek kalıcı ve büyük maddi zararlara yol açan veri kayıpları da sağladı. Ayrıca BT sunucularına bağlanarak DDoS saldırısı ile çağrı merkezini işlemez hale getirdi ve abonelerin dağıtım merkezi ile irtibata geçmesinin de önüne geçmiş oldu. Bu da elektrik kesintisinin daha uzun bir süre etkisini sürdürmesi için yeterliydi.

Saldırı aşamalarından kısaca bahsetmek gerekirse; 1. Aşamada birden çok kullanıcıya BlackEnergy uygulamasının bulunduğu hedefli oltalama postasının gönderilmesi ve bu postanın çalışanlardan birinin etkileşime geçmesiyle birkaç gün sürmüş ve aylarca sürecek dinleme aşaması için kurumun iç ağına adım adım yayılmıştır. 2. Aşama 5 ay gibi bir sürede pasif dinleme aşaması olarak sürdürülmüştür. Son aşama ise en kısası ve saldırının gerçekleştiği 3. aşamadır. Bu aşamada doğru zamanda sistemler kilitlenerek sadece 10 dakika içerisinde tüm saldırı gerçekleşti.

Saldırının tüm üç aşaması ile ilgili analiz tam olarak yapılamadı, çünkü saldırganın sildiği veriler sayesinde sistem üzerindeki günlük kayıtlarının da çoğu kalıcı olarak silindi. Bu saldırıyı önemli kılan 2 büyük faktör vardır; birincisi çok sayıda farklı siber saldırı yöntemi bir arada kullanılarak kritik altyapı üzerinde tahribat maksimum seviyeye çıktı, ikincisi ise Rusya merkezli hacker grubu tarafından gerçekleştirilen bu saldırı ile Kırım krizi sonrası patlak veren Ukrayna – Rusya krizine yeni bir boyut kazandırdı.

Ayrıca elektrik üretim şebekelerinin ne kadar büyük bir risk altında olduğunu daha net görebilmemiz için, Dünya üzerindeki tüm elektrik şebekelerinin %91'inin en az bir siber saldırı yaşadığını bu vesile ile hatırlatmakta fayda var.[12]

NotPetya Saldırısı - 2017

2017 yılının Haziran ayında, Ransomware yöntemi kullanılarak yapılan NotPetya Saldırısı mağdurlarına vermiş olduğu 10 milyar ABD Doları zarar ile günümüze kadar gerçekleştirilmiş en büyük ekonomik etkiye sahip siber saldırı niteliğini taşımaktadır. Yine başta Ukrayna'yı hedef alan bu saldırı daha sonra kontrol edilemez bir hale gelerek tüm Dünya genelinde pek çok ülkeye hızla yayılmıştır.

Saldırının kaynağı olarak Ukrayna'da yer alan Linkos Group kuruluşuna ait M.E.Doc vergi hesaplama uygulaması gösterildi. Uygulama, Ukrayna'da ticaret yapan ve vergi sistemine dahil olan tüm kurumlar tarafından kullanılıyordu. Virüsün sistemlere bulaşması ise, M.E.Doc uygulamasına yapılacak bir güncelleme yaması sayesinde yaşandı. Rusya merkezli olduğu düşünülen hacker grubu bu güncelleme paketinin içine sızarak ransomware yazılımını yerleştirdi ve güncelleme yapan tüm kurumlar hızla virüsü sistemlerine dahil etti. Virüsün bu kadar fazla tahribat yaratmasındaki temel sebep ise, Microsoft işletim sistemlerinde kullanılan mesajlaşma protokolü SMB içerisinde yer alan bir açık sayesinde hem kullanıcı kurumdaki tüm ağ sistemine hem de kurumlarla bağlantılı üçüncü kişi ve kurumların sistemlerine hızla yayıldı. Ayrıca bu yönüyle NotPetya saldırısı en kısa sürede en fazla alana yayılan siber saldırı olma özelliğini taşımaktadır.

[12] Bayar, T. (2014, Oct. 14). Cybersecurity in the power sector. Power Engineering International, Vol. 22/#9.

Saldırı sızdığı sistemlerde bir ramsomware uyguladı ve sunucularda yer alan tüm verileri geri döndürülemez şekilde şifreleyerek büyük miktarda veri ve maddi kayıplara yol açtı. NotPetya saldırısının en fazla zarar gören mağdurları arasında Merck, Fedex, Saint-Gobain ve Maersk gibi global kurumlar yer alıyor. Saldırı nedeniyle başta Maersk olmak üzere pek çok kurumun lojistik tedarik zincirinde yer alan süreçler işlemez hale geldi. Dünyada oldukça önemli yer tutan New Jersey ve Mumbai ticaret limanlarında Maersk kurumuna ait tüm ticaret ve lojistik faaliyetleri sorun çözülene kadar bir süreliğine durduruldu.

Estonya Saldırısı - 2007

Estonya bir siber saldırının ülke geneline uygulandığı ve siber savaşın kamu kaynakları, resmi kurumlar, bankalar ve sağlık hizmetleri başta olmak üzere ülke genelinde kendisini gösterdiği ilk ve en açık saldırıdır. 2007 yılında ülkede yaşanan Rusya kaynaklı bazı siyasi karışıklıklar sonrasında birkaç hafta boyunca süren yoğun DDoS saldırısıyla karşı karşıya kaldı. Normalde bu tarz DDoS saldırı o zamana kadar sadece birkaç gün süren manipülasyonlar halinde uygulanırdı veya sadece belli bir kurumu hedef alırdı. Estonya'ya yapılan bu saldırılarda haftalarca süren yoğun ve aralıksız saldırılar sonucunda hükümet, kamu hayatının devam etmesinin imkansız hale gelmesi ile bunu bir savaş eylemi olarak tanımladı ve üyesi olduğu NATO'dan yardım istedi. Saldırıyı özel kılan bir diğer önemli nokta ise, bu saldırı sonrasında NATO siber saldırıyı da diğer saldırılardan farksız bir tehdit olarak kabul ederek ittifakın siber savunma birimi olan CCDCoE kuruluşunu kısa süre içerisinde 2008 yılında merkezi Estonya başkenti Talinn olacak şekilde ilan etti.

Saldırının uluslararası bir boyut kazanması ile birlikte uluslararası uzmanlardan oluşan bir ekip, bu saldırıya dair geniş çaplı bir inceleme gerçekleştirdi. Elde edilen bulgulara göre ABD, Kanada, Brezilya, Vietnam gibi ülkelerin sunucularının saldırı esnasında kullanıldığı ortaya çıktı. Bulgular saldırının sorumlusu olarak Rusya'yı işaret etmekteydi ancak bu husus, Rus resmi makamlarca hiçbir zaman doğrulanmadı. Bir diğer ilginç bulgu ise ise Estonya kurumlarının aldığı internet trafiğiydi. Saldırı öncesi günlük 1000 civarı ziyaret alan çeşitli kurumlar saldırı süresince DDoS atakları sayesinde saniyede 2000 üzerinde ziyaret aldıkları tespit edildi. Bu rakam küçük bir ülke olan Estonya kurumlarının hizmet kapasitesini ve dolayısıyla internet trafiğinin kaldırabileceği yoğunluğun fazlasıyla üzerinde. Bu kadar yüksek saldırı karşısında ülkedeki başlıca kurumların sunucu altyapıları taleplere karşılık veremez hale geldi ve sunucu sistemleri çöktü. Daha fazla tahribat yaşanmaması adına saldırılar devam ederken Estonya hükümeti, ülkenin tüm internet trafiğini dış dünyaya kapattı ve yurt dışı merkezli olduğunu düşündükleri saldırıların çoğunu engellediler.

Bu saldırı ile birlikte siber saldırıların kitle imha silahları kadar tehlikeli boyutlara ulaşabileceği sonucuna varıldı. Sadece bu saldırının NATO üyesi bir ülkeye yaşanması ile birlikte NATO siber savunma için ciddi bir bütçe ayırarak hizmet vermeye başladı ve ülkeleri hedef alan, kritik altyapı ve kamu kaynaklarını işlemez hale getiren siber saldırılar savaşın başka bir boyutu olarak kabul gördü. Ayrıca bu kapsamda NATO, düzenli olarak her yıl Locked Shields adını verdiği siber savunma tatbikatını düzenlemektedir. 2010 yılından beri aralıksız düzenlenen tatbikatların sonuncusu bu yıl Nisan ayı içerisinde siber savunma merkez üssü olan Talinn'de 24 tanesi üye ülke olmak üzere 33 ülkeden 2000 katılımcı ile 3 gün süresince gerçekleştirildi.[13]

[13] NATO, Exercise Locked Shields 2022 Concludes, https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022-concludes, 23 April 2022

Yapay Zeka & Büyük Veri Destekli Teknolojilerin Gelişimi

Dünya çapında, verinin ilk saklandığı andan 2020 yılına kadar veri dünyasını 5.9 Zettabayt (1 ZB = 1 Milyar TB) tekil ve benzersiz veri oluştururken 2024 yılına kadar sadece 4 yıllık bir sürede benzersiz veriler 7.51 Zettabayt artış ile 13.41 Zettabayt seviyesine ulaşacağı ifade edilmektedir.[14] Yani çeşitli büyük veri ve yapay zeka uygulamalarında kullanmak üzere 4 yıllık süre içerisinde 2.27 kat daha fazla veri saklanacak ve bir o kadar daha fazla verinin saldırıya uğramaması için gerekli tedbirleirn alınması gerekecek. Veri ölçeğinin bu kadar hızlı büyümesi tecrübeli ve yeterli bilgi birikimine sahip siber güvenlik uzmanı ihtiyacını arttıracak. Bu durumda uluslar, vatandaşlarının eğitim ve yetkinliklerini geliştirerek hem nitelikli personel kazanmak hem de istihdam arttırmak için iyi bir fırsat yakalayacak. Fakat operasyonel hale gelen iş yükünün artması, sürekli yeni tehditlerin ortaya çıkması, beyin göçü, otomasyon ihtiyacı ve kritik sistemlerde sıfır duruş süresi gibi yüksek performans gerektiren durumlar bir yandan da kişi bağımsız, otomatize edilmiş yapay zeka destekli sistemleri cazip hale getiriyor.

Yapay zeka kullanımını cazip kılan bir başka sebep; yaşanan olası bir siber güvenlik saldırısı yada veri ihlali durumlarında zararı minimuma indirebilmesidir. 2021 yılı itibari ile dünya çapında ortalama bir veri ihlalinin maliyeti kurumlar için 3.86 Milyon ABD Doları olarak kabul ediliyor.[15] Yapay zeka destekli sistemler daha az güvenlik aracı kullanımı ile uygulama bağımlılığını azaltırken, insan müdahalesini de ortadan kaldırarak hata payı ve personel maliyetlerinde de büyük düşüş sağlıyor. Bu sistemler, izinsiz giriş, hedefli oltalama saldırıları[16] ve sahtekarlık tespiti gibi konularda sağladığı otomasyon ile ön plana çıkıyor. Günümüzde yapay zeka destekli kurumların yaşadığı ortalama bir veri ihlalinin maliyeti diğer kurumlara göre %25 daha azdır (2.9 Milyon ABD Doları).[17] Ayrıca, yapay zeka destekli sistemler klasik sistemlere göre bir saldırının tespiti ve kontrol altına alınması konusunda %27 daha hızlıdır.[18]

Aşağıda kritik altyapının farklı hizmet alanlarına ait yaşanabilecek siber saldırılarda yapay zekanın kullanım örneklerine yer verilmiştir.

Bankacılık & Finans:	Fon & Borsa Yönetimi[19] = Anomali Tespiti.
Sağlık:	Robotik Cerrahi[20] & Sağlık Kayıt Sistemi = Anomali& Arıza Analizi.
Ulaşım Sistemleri:	Trafik Kontrol Sistemleri & Otopilot[21] = Arıza Analizi, Yüksek Erişilebilirlik.
Kamu Yönetimi:	E-Devlet = Sahtekarlık, İzinsiz Giriş Tespiti.

[14] Statista, Share of unique data and replicated data in the global datasphere in 2020 and 2024, https://www.statista.com/statistics/1185888/worldwide-global-datasphere-unique-replicated-data/ , (1 November 2020)
[15] Statista, Cyber Crime & Security [web page], https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#overview
[16] U. Ozker & O.Sahingoz, Content Based Phishing Detection with Machine Learning, https://ieeexplore.ieee.org/document/9249892 , (9 November 2020)
[17] IBM, Data Breaches Report 2021 p:35, https://www.ibm.com/downloads/cas/OJDVQGRY
[18] IBM, Data Breaches Report 2021 p:39, https://www.ibm.com/downloads/cas/OJDVQGRY
[19] Yuan Qi and Jing Xiao. "Fintech: AI powers financial services to improve people's lives." Communications of the ACM 61.11 (2018): 65-69
[20] Danny Lange, "Cognitive Robotics," to appear in IEEE Computer, December 2019
[21] Andrew J. Hawkins, "Deadly Boeing Crashes Raise Questions About Airplane Automation," The Verge, https://www.theverge.com/2019/3/15/18267365/boeing-737-max-8-crash-autopilotautomation, March 15, 2019

DÜNYADA YAPILAN ÇEŞİTLİ ÇALIŞMALAR & DÜZENLEMELER

Avrupa Birliği Tarafından Gerçekleştirilen Çalışmalar

Avrupa Birliği Siber Güvenlik Yasası

Avrupa Birliği (AB) artan siber güvenlik endişeleri ile birlikte ortak bir vizyon ve misyon geliştirme amacıyla bir Siber Güvenlik Yasası kabul etmiştir. Bu yasanın yürürlüğe girmesi ile birlikte, ortak siber güvenlik politikasının geliştirilmesinde, uygulanmasında ve gözden geçirilmesinde Komisyon'a ve üye devletlere sorumluluk verilmektedir. Anılan yasa, uygulayıcı kurum olarak ENISA'yı öne çıkarmakta ve merkezi bir siber savunmanın geliştirilmesi, standartların ve sertifikasyonların ortaya konması ve yürütülmesinde tavsiyeler sağlayarak farkındalığı arttırmaktadır. ENISA yasanın yürürlüğe girmesi sonrasında AB kurumlarının ve organlarının siber güvenlik hakkında bilgi edinmek için başvuracağı merci konumuna gelmiştir.

Ayrıca ENISA, AB düzeyindeki olay müdahale ekiplerinin yönetiminden (CSIRT) sorumlu olacak ve üye devletlere siber saldırılara karşı yardım sağlamakla mükellef olacaktır.

Avrupa siber güvenlik sertifikasyon programları ise; ENISA yönetiminde, uzman tavsiyeleri, sektör paydaşları, AB Komisyon Üyeleri ve AB Üye Devletleri'nin katılımı ve yakın işbirliği ile hazırlanacak ve kabul edilecektir.

Siber güvenlik sertifikasyon programı kabul edildikten sonra, BİT ürünleri üreticileri veya BİT hizmetleri sağlayıcıları, ürünlerinin veya hizmetlerinin sertifikalandırılması için başvuruları kendi seçtikleri uygunluk değerlendirme kuruluşuna sunabilmektedir. Kanun ayrıca, çevrimiçi hizmetlerin ve tüketici cihazlarının siber güvenliğini artırarak, siber güvenlik sertifikası için bir AB çerçevesi de oluşturmaktadır.

Yeni bir sertifikasyon süreci başlatma kararı alındığı zaman öncelikle AB üye ülkelerinden oluşan AB Siber Güvenlik Sertifikasyon Grubu, komisyona sertifikasyon talebini iletir ve komisyon aracılığı ile ENISA'dan süreci başlatması istenir. ENISA, AB Üye Ülkelerinden uzmanlar, sektör katılımcıları ve danışmanların olduğu bir işbirliği grubunu çalışma için bir araya getirerek sertifikasyon geliştirme ve düzenleme süreçlerini uçtan uca yürütür. Son aşamada hazırlanan program AB Komisyonu'na teslim edilir ve komisyon programı kabul ederek yürürlüğe koymak üzere süreci tamamlar.

5G Dönüşümü Kapsamında AB Siber Güvenlik Yaklaşımı

5G, günümüz innovasyon ortamlarının gelişmesi sonucu daha hızlı, performanslı ve günlük hayatımızda çok daha fazla sürecimizi internet ortamına taşıyabileceğimiz bir hizmet ihtiyacına karşılık vermek için bugünlerde hayatımıza dahil oluyor. AB üye ülkeler arasında sınırsız veri ve teknoloji kullanımı için merkeze konumlandırdığı Dijital Tek Pazar Stratejisi'nin bir başlığı olarak siber güvenlik ağırlıklı 5G Eylem Planı'nı kabul etmiştir.[22] 5G ağları kullanıma sunulduğunda, iç pazarın işleyişi ve enerji, ulaşım, bankacılık ve sağlık gibi hayati toplumsal ve ekonomik işlevlerin sürdürülmesi ve işletilmesi için gerekli olan geniş bir hizmet yelpazesinin bel kemiğini oluşturacaktır. Birçok kritik hizmetin 5G ağlarına bağımlılığı, sistemik ve yaygın bozulmanın sonuçlarını özellikle ciddi hale getirecektir. Sonuç olarak, 5G ağlarının siber güvenliğinin sağlanması, siber saldırıların arttığı ve her zamankinden daha karmaşık olduğu bir zamanda AB için stratejik öneme sahip bir konudur. Dijital ekosistemi destekleyen altyapıların birbirine bağlı ve uluslararası doğası bir üye devlette 5G ağlarıyla ilgili herhangi bir önemli güvenlik açığı veya siber güvenlik olayının tüm AB ülkelerini etkileyeceği anlamına gelir. Bu nedenle, 5G ağlarının yüksek ölçekte ortak bir siber güvenlik düzeyini desteklemek için önlemler alınması zorunlu hale gelmiştir. Ayrıca, stratejik

[22] European Commission, Digital Single Market Strategy Document, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192 , 06.05.2015

sektörlerde yabancı yatırım, kritik varlıkların, teknolojilerin ve altyapının satın alınması ve kritik ekipmanların üçüncü parti sağlaycılar tarafından tedarik edilmesi de risk oluşturabilir.

ENISA, Avrupa Komisyonu, AB Üye Devletler ve ulusal düzenleyici makamlar 5G ile gelen risklere bağlı olarak bazı düzenlemeler geliştirmişlerdir.[23] Bu süreçte piyasa oyuncuları, sektör paydaşları ve akademisyenler de geçici çalışma grupları başlığı altında yönergelerin geliştirilmesi sürecinde danışmanlık hizmeti sağlayarak aktif rol almışlardır. Getirilen düzenlemeler içerisinde en dikkat çekici noktalardan biri; AB Genel Veri Güvenliği Kanunu[24], kapsamında 5G ağı dahilinde IOT ve benzer sistemlerin kullanımının artmasıyla birlikte daha fazla verinin hayatımıza dahil olacağı ve kişisel verilerin korunmasının önemi ile yetkisiz kişi yada kuruluşların erişiminin doğuracağı olası sonuçlara değinilmiştir. Kişisel ve hassas verilerin korunmasının eskisinden çok daha önemli ve zor olduğu ortamlarda ek risk yönetim ve kontrol yapılarının uygulamaya alınması gerekmektedir. Bu kapsamda, AB içerisinde genel bir risk değerlendirme yapısı geliştirmek için; ortak önlem grubunu belirlemek üzere AB İşbirliği Grubu Direktifi [25] kapsamında kurulan çalışma grubu ile tedarik zinciri riski (NotPetya Saldırısını anlattığımız bölümde tedarik zinciri üzerindeki etkilerine değinilmişti), yazılım güvenlik açığı riski, erişim kontrolü riski, BT kaynaklı diğer riskler değerlendirilerek risk yönetim süreçleri de 5G sertifikasyon süreçlerine entegre ve AB dahilinde tek bir merkezden yönetilecek biçimde ortaya konmuştur.

Enerji Şebekeleri Kapsamında Kritik Altyapının Önemi

Kritik enerji altyapısı, enerjinin üretim, dağıtım, tedarik ve depolanmasında kullanılan tüm sistemleri temsil etmektedir. Kritik enerji altyapı paydaşları; elektrik üretim, dağıtım ve iletim, yakıt olarak kullanılan maddelerin (kömür, LPG, LNG, Petrol, nükleer enerji ham maddeleri, yenilenebilir enerji kaynakları (rüzgâr, güneş, hidroelektrik) santrallerde üretilmesini, işlenerek son kullanıcı ürünü haline getirilmesini ve tüketiciye kadar ulaştırılmasını sağlayan her türlü tesis ve bu tesislerde süreçlerin yönetilmesini ve güvenliğini sağlayan sistemler, kritik enerji altyapısının bileşenleridir. Nitekim EPDK da bu kapsama uygun şekilde kritik enerji altyapısını; "İşlevlerini kısmen veya tamamen, yerine getiremediğinde, toplumsal düzenin sürdürülebilirliğinin veya kamu hizmetlerinin sunumunun olumsuz etkileneceği enerji ağı, varlığı, sistemi ve yapılarının bütünü"[26] olarak tanımlamaktadır. Enerji şebekelerinde kritik altyapı paydaşlarının herhangi bir siber saldırıya uğraması durumunda olası etki ve sonuçları, diğer alanlardaki kritik altyapı varlıklarının saldırıya uğramasına göre çok daha etkili ve yıkıcı olabilmektedir. Bir siber saldırı durumunda; fiziksel altyapının zarar görmesi, ülkelerin ulusal güvenliğinin tehdit altına girmesi, vatandaşların maddi – manevi tahribat altında kalması, kurumların yükümlülüklerini yerine getiremez hale gelmesi, kurum yada kişilerin büyük ölçekte finansal kayıplar yaşaması, enerji pazarında sonucu uluslarası ölçekte hissedilebilir arz – talep dengelerinin bozulması gibi pek çok güçlü ve yıkıcı etki aynı anda hissedilebilir.

Kritik altyapıyı etkileyen saldırıların %79,32'lik büyük bir kısmı doğrudan enerji sektöründe yer alan varlıkları hedef almaktadır.[27] Enerji sektörünü hedef alan saldırıların her geçen gün daha da artarak devam etmesi beklenmektedir. Bunun başlıca sebebi; elektrik, petrol, gaz, nükleer ve diğer yenilenebilir hizmetler, şebekelerini çalıştırmak için otomatik kontrollere giderek daha fazla veri bağımlı hale gelmişlerdir. Bu altyapı sistemleri bugünlerde IOT sensörlerinde desteği ile birbirine bağlı ağ sistemleri aracılığıyla tam otomatik kabiliyetlerle yönetilip otomasyona dahil edilmiştir. Pek çok modern enerji üretim tesisi ve kuruluşlar sayaçları yönetmek ve müşterilerinin verilerini analiz etmek için veri ağlarına

[23] https://resilience.enisa.europa.eu/article-13
[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.
[25] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p.1).
[26] Türkiye Official Newspaper, https://www.resmigazete.gov.tr/eskiler/2017/07/20170713-5.htm, 13.07.2017
[27] Defender, Defending the European Energy Infrastructures, CEI Security Stakeholder Group Manifest – Deliverable 6.2, P:7, 07.11.2017

güvenirler. Buna operasyonel süreçleri de dahil edersek, tesisleri yönetmek için kullanılan kontrol odaları, trafo merkezleri, cihazlar, rafineriler ve boru hatları artık tamamen dijital, video etkin, yüksek hızlı veri bağlantılarına dayanmaktadır.

Veri ve analitik merkezli enerji üretim tesisleri yukarıdaki süreçleri yönetmek için kaynak dağıtımı, üretim optimizasyonu, güvenlik kontrolü, önleyici bakım ve tedarik zinciri planlama gibi temel süreçlerinde genellikle son yıllarda kazandıkları dijital yetkinlikleri ve analitik araçları kullanmaktadır. Bu sebeple dijitalleşme, enerji sektörünü giderek artan bir şekilde siber saldırılar için daha fazla potansiyel hedef haline getirmektedir. Öncelikle dijital ve büyük veri odaklı sistemler veri ihlallerine veya hırsızlığa maruz kalabilecek daha yüksek hacimde veri oluşturur. Örneğin, bir petrol rafinerisi sadece bu süreçleri sürdürmek için günde 1 terabayt veya çok daha fazla miktarda ham veri üretir[28]. Sistemlerde yaşanabilecek olası bir saldırı veya sızma ile bu verinin içerisindeki sadece 1 karakterlik kısmında bile yapılacak küçük bir değişiklik, tüm operasyon sürecinin durmasına ve geri dönüşü olmayan kayıplar yaşanmasına neden olabilir.

Eurobarometer kamuoyu araştırması[29], AB vatandaşlarının %86'sının da güvenli enerjiye erişimi sağlamak için AB ülkeleri arasında enerji başta olmak üzere siber güvenlik konusunda daha fazla işbirliği olması gerektiği konusunda hem fikir olduğunu göstermektedir. Bu kapsamda AB üye ülkeleri ve AB Komisyonu lideriliğinde, NATO Enerji Güvenliği Mükemmeliyet Merkezi'nin de (ENSEC COE) katılımıyla, her bir ortak ülkenin ve hatta özel şirketlerin enerji başta olmak üzere kritik altyapılarında meydana gelebilecek yeni siber saldırı tehditlerini daha geniş araştırma ve geliştirme imkanlarıyla buluşturmak için önemli bir görev üstlenmektedir.

NATO'nun Terörizme Karşı Savunma Mükemmeliyet Merkezi'ne (COEDAT) ev sahipliğini yapan ülkemiz ise kritik enerji altyapılarının siber saldırılara karşı korunmasında daha geniş bir rol oynamak durumundadır. Ayrıca, sahip olduğu coğrafya üzerinden geçen uluslararası öneme sahip TANAP, TürkAkım, Bakü-Ceyhan-Tiflis Petrol Boru Hattı, Irak-Türkiye Ham Petrol Boru Hattı gibi önemli altyapı projeleri göz önünde bulundurulduğunda, Türkiye %4 siber saldırı oranı ile enerji sektöründe saldırılardan en çok etkilenen dünyada 11. NATO ülkeleri arasında ise 5. ülke konumunda olması hiç şaşırtıcı değildir. Türkiye, bu alanda hem liderliği üstlenip hem de yapacağı işbirlikleri ile başta AB olmak üzere dünyaya rol model olma potansiyeli taşımaktadır.

Sağlık Sektöründe Kritik Altyapının Önemi

Kritik sağlık altyapısı, bugün kamu sağlığı ile ilişkilendirilen özel/devlet hastaneleri ve sağlık kuruluşları, her türlü amaçla kullanılan sağlık ve bakım destek teçhizatları, ilaçlar, sağlık veri tabanları, medikal ürünler, sağlık bilgi sistemleri ve bunlara bağlı endüstriyel kontrol sistemlerini kapsamaktadır. Dijital dönüşüm ve COVID-19 pandemisinin etkisiyle birlikte günümüzde E-Sağlık dönüşümü çerçevesinde sağlık alanında pek çok hizmet gelişen teknoloji ve bulut hizmetlerin sağladığı imkanlarla uzaktan ya da ham veri üreten cihazlar tarafından gerçekleşmektedir. Şu anda tıbbi teknoloji şirketleri tarafından sağlanan sağlık hizmetleri giderek daha fazla birbirine bağlı ve yaygın hale gelmektedir. Yaygın olarak kullanılan giyilebilir cihazlar gibi 500.000'den fazla farklı türde tıbbi cihaz ve teçhizat bulunmaktadır.[30] Bu kadar hızlı bir sektörel büyüme sayesinde sektörün ekonomik boyutu da hızla artan bir ivme göstermektedir. 2017 yılında tıbbi teknoloji pazarının kabaca 115 milyar ABD doları seviyesindeyken, 2022 yılı sonlarına gelindiğinde 5 yıllık sürede yaklaşık 4 kat artış göstermesi öngörülmektedir.[31]

[28] Journal of Petroleum Technology, 2012: Data Mining Applications in the Oil and Gas Industry
[29] Eurobarometer 492, https://europa.eu/eurobarometer/surveys/detail/2238, 01.02.2019
[30] Deloittle, Life Sciences for Health Care, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomtbrochure.pdf
[31] MedTech Europe, The European Medical Technology Industry ib Figures 2019, https://www.medtecheurope.org/wp-content/uploads/2019/04/The-European-Medical-Technology-Industry-in-figures2019-1.pdf

Sağlık sektöründe kritik altyapının önemi ise, 2017 yılında yaşanan WannaCry siber saldırısı sonrasında ön plana çıkmıştır. Bu kadar çok sayıda elementin bir arada yer aldığı, kompleks ve her geçen gün daha fazla dijital dünya ile entegre bir sağlık servisinin siber saldırıların hedefi olması yada etkilenmesi şaşırtıcı olmamıştır. Birleşik Krallık Ulusal Sağlık Sistemi, WannaCry saldırısının kurbanı olarak çok sayıda sorun ile karşı karşıya kalmıştır. Başlıca sorunlardan bahsetmek gerekirse; 19.494 adet hasta randevuları ve operasyonları iptal edilmiş, çok sayıda tıbbi cihaz saldırıdan etkilenerek kilitlenmiş ve işlevsiz hale gelmiştir.[32] Pek çok hastanın tahlil ve test sonuçlarının tesliminde sorunlar oluşmuştur. Ayrıca, Ulusal Sağlık Sistemi'ne bağlı ya da entegrasyonu bulunan kamu ile ilişkili çok sayıda organizasyon veri alışverişinde ve USS verilerine erişimde sıkıntılar yaşarken, veri sızıntıları da meydana gelmiştir. Saldırı kontrol altına alınana kadar 12 – 19 Mayıs 2017 tarihleri arasında 7 gün süreyle sistemlerde ciddi sorunlar yaşanmıştır. Bu saldırılarda tek iyi taraf can kaybının yaşanmaması belki de, fakat her siber saldırının sonuçları aynı olmayabilir. Özellikle sağlık sektöründe yaşanan siber saldırılar insan ölümleri ile sonuçlanmaya en yakın tür diyebiliriz.

2020 yılında daha ufak çaplı bir fidye yazılımının Düsseldorf Üniversite Hastanesi sunucularını hedef alması sonucu medikal cihazlarda yaşanan bozulmalar sebebiyle Alman bir kadın hayatını kaybetmişti.[33] Özellikle Birleşik Krallık Ulusal Sağlık Sistemi'ni 1 hafta boyunca etkileyen WannaCry ve Almanya'da ölümle sonuçlanan siber saldırı sonrasında AB üye devletleri ve Komisyonu, enerji alanında olduğu gibi sağlık alanında da kritik altyapıyı etkileyen siber saldırılara karşı pek çok regülasyon, eğitim, sertifikasyon ve SOME gibi süreçleri dahil ederek sağlık kuruluşlarında yaşanabilecek siber saldırılara karşı koruma poltikalarını oluşturdular. Bu süreçte GDPR ve NISD sağlık sektörünü de kapsayacak şekilde güncellendi ve medikal cihazlar özelinde MDR regülasyonu oluşturularak devreye alındı.

AB ve üye ülkeler, sağlık alanında yaşanacak herhangi bir siber saldırı olayına karşı hedef olabilecek kaynakları 10 alt başlığa ayırmıştır. Uzaktan bakım sistemleri, tanımlama sistemleri, mobil hasta cihazları, medikal cihazlar, bulut servisler, klinik bilgi sistemleri, profesyonel hizmetler, endüstriyel kontrol sistemleri, hastane bilgi sistemleri, ağ ekipmanları olarak gruplanan sağlık sektörü; etki alanı, boyutu, oluşabilecek zararlar ve teknik altyapıları açısından değerlendirilerek gruplandırılmıştır.

Ayrıca, Mart 2022 tarihinde Horizon 2020 desteği ile kurulan Panacea[34], siber güvenliğin yalnızca finansal olarak değil, aynı zamanda bir hizmetin operasyonel sürekliliğini tehdit ederken hasta güvenliğini ve kişisel sağlık verilerini de riske attığı için sosyal olarak da alakalı olduğunu benimseyerek işbirliği, veri paylaşımı, eğitim ve bilinçli siber güvenlik amacı ile kurulmuştur. Organizasyon, sağlık hizmetlerinde siber güvenlik için entegre bir çözüm olarak bir araç seti geliştirerek, sağlık kuruluşlarının siber güvenlik hazırlıklarını ve dayanıklılıklarını değerlendirmelerine ve iyileştirmelerine yardımcı olmaktadır. Bu araçlar birbiri ile senkronize olarak; teknoloji, insanlar ve süreçler genelinde siber güvenliğe çok yönlü, kuruluş çapında bir yaklaşım sağlar. Araç setini çok uzun zaman olmamasına rağmen AB sınırları içerisinde farklı ülkelerden 15 üniversite hastanesi partner olarak desteklemekte ve sağlık alanında kritik altyapıların güçlendirilmesine destek sağlamaktadır.

Türkiye, birçok AB ülkesine oranla daha yüksek olan nüfusu ve geniş coğrafyası ile Panacea gibi AB ülkeleri özelinde üniversite hastanelerinin katıldığı organizasyonlara üniversite hastaneleri seviyesinde katılarak kendi ülkesinin sağlık altyapısını koruması adına fayda sağlayabilir. Keza, bu tarz girişimlerin ortaya çıkması amacıyla sağlık sektörü paydaşları ile girişimcilerini destekleyerek Horizon 2020 gibi programlarda siber güvenlik ile sağlık alanında daha aktif roller alınmasını sağlayabilir.

[32] NAO, Investigation WannaCry cyberattack and the NHS, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf, 01.10.2017
[33] NewYork Times, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html
[34] https://www.panacearesearch.eu/

Finans Sektöründe Kritik Altyapının Önemi

Kritik finans altyapısı, bankacılık kuruluşları, ödeme sistemleri, finansal teknoloji girişimleri, çeşitli ölçekte tüm borsa kuruluşlarını ve son dönemlerde tüm dünyada alternatif finansal varlık olarak kullanılan kripto para kuruluşlarını kapsamaktadır. Son yıllarda, finans sektöründe finansal teknoloji alanındaki fırsatların büyümesi, sektör hacminin genişlemesi, yeni dinamiklerin oluşması, klasik bankacılık süreçlerinin çevrimiçi alternatifleri ile yer değiştirmesi gibi gelişmelerle birlikte finansal kritik altyapı sistemlerine yapılan siber saldırılarda kayda değer bir artış meydana gelmektedir. Trend Micro'nun raporuna göre, yalnızca 2021'in ilk yarısında bankacılık sektöründeki fidye yazılımı saldırıları, diğer sektörlerle orantısız olarak %1318 gibi büyük bir artış gösterdi.[35] Siber saldırılarda yaşanan bu artış ile birlikte finans şirketleri diğer sektörlerden 300 kat daha fazla hedef haline gelmiştir[36], bu sektörün siber suçlular için ne kadar çekici olduğunu açıkça göstermektedir. Hala gelişmeye devam eden iki eğilim bu riski daha da artırmaktadır. Birincisi, küresel finans sistemi, COVID-19 pandemisi tarafından hızlandırılan eşi görülmemiş bir dijital dönüşümden geçmektedir. Bankalar teknoloji şirketleriyle rekabet etmekte, teknolojişirketleri de bankalarla rekabet etmektedir. Bu arada, pandemi çevrimiçi finansal hizmetlere olan talebi artırmış ve evden çalışma düzenlemelerini norm haline getirmiştir. Merkez Bankaları, bir yandan kendi kontrollerindeki dijital paraları hayata geçirmeyi planlamakta diğer yandan ödeme sistemlerini modernleştirmeye çalışmaktadıri. İkincisi, kötü niyetli aktörler bu dijital dönüşümden yararlanmakta ve küresel finansal sistem, finansal istikrar ve sistemin bütünlüğüne olan güven için büyüyen bir tehdit oluşturmaktadır.

TEHDİT EDEN	MOTİVASYON	AMAÇ	SALDIRI TİPİ
Ulus Devletler, Ulus Destekli Gruplar	Jeopolitik, İdeolojik	Finansal Kazanç, Hırsızlık, Casusluk, Siyasal İstikrarsızlık, Ulus Ekonomisi Tahribatı, Ulusal Tahribat	Kalıcı Veri Kaybı, Ödeme Sistemleri Kesintisi, Hileli Transferler, Casusluk
Siber Suçlular	Haksız Kazanç	Hırsızlık	Nakit Hırsızlığı Hileli Transferler, Kimlik Hırsızlığı
Terörist Gruplar, İç Tehditler	İdeolojik	Siyasal Deformasyon, Ekonomik Tahribat	DDoS Saldırısı, Sızma Girişimi, Sahtekarlık

Tablo – 1

Tablo - 1[37]'de finans sektöründe kritik altyapıları tehdit eden farklı aktörleri, sahip oldukları motivasyonları, amaçlarını ve kullandıkları saldırı yöntemlerinin sınıflandırması gösterilmektedir. Günümüzde, finansal sistemlere yapılan saldırılar ile haksız kazanç elde etmek, siyasi ve ideolojik sonuçlar sağlamak gibi kazanımlar sağlamak, bu alana yapılan siber saldırılardaki artışın bir diğer sebebi olarak kabul edilebilir.

Finans sektöründe yapılan siber saldırılar son 10 yılda çok ciddi ve tehlikeli bir boyuta ulaşmıştır. Bu alanda yapılan siber saldırılar bankalar arası fon transfer hizmeti SWIFT servisini hedef alacak kadar ileri gidebilmektedir. 2016 ve 2018 yıllarında Kuzey Kore merkezli ve SWIFT üzerinden doğrudan Malezya ve

[35] TrendMicro, Attacks Surge in 2021, https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats, 14.09.2021
[36] Boston Consulting Group (2019). Global Wealth 2019: Reigniting Radical Growth.
[37] ESRB, MI5 and Cambridge Centre for Risk Studies.

Hindistan Merkez Bankalarını hedef alan saldırılar, işlemler gerçekleşmeden önce sistem tarafından tespit edilerek başarısızlıkla sonuçlanmıştır.[38] Fakat benzer bir saldırı Bangladeş Merkez Bankası'nı zarara uğratmıştır.

Bangladeş Merkez Bankası hedef alınarak 04 Şubat 2016'da gerçekleştirilen saldırı tarihin en büyük ve en etkileyici siber soygunlarından biridir. Soygunu etkileyici kılan SWIFT sistemi üzerinden profesyoneller tarafından gerçekleştirilen saldırı ile doğrudan bir ülkenin merkez bankasının parası çalınmıştır. Soygunu büyük kılan ise, çalınan paranın 81 milyon ABD Doları tutarında olmasıdır. Muhtemelen aylarca süren hazırlıktan sonra, organizasyonel ve teknik olarak, sistemlere sızma, pasif uzun süreli izleme, kimlik bilgileri edinme gibi farklı saldırı yöntemlerini bir arada hibrit olarak kullanan saldırganlar, Federal Rezerv'e 35 adet sahte para transferi talebi gönderdi. New York Bankası gelen sahte para transferi talebine istinaden, Bangladeş Bankası'nın VOSTRO hesabında bulunan milyonlarca doların Filipinler, Sri-Lanka ve Asya'nın diğer bölgelerindeki banka hesaplarına transfer etmesini istedi. Saldırganlar, Filipinler'deki Rizal Commercial Banking Corporation'a (RCBC) 4 sahte transfer talebiyle 81 milyon ABD Doları, Sri-Lanka'ya ise tek bir istek ile ek 20 milyon ABD Doları göndermeyi başardı. Geri kalan diğer 30 sahte transfer talebi Fed tarafından erken aşamada tespit edilerek 850 milyon ABD Doları tutarındaki hırsızlık önlenebildi. Filipinlere 4 parça halinde gönderilen 81 milyon ABD Doları, aynı gün içerisinde üç farklı hesaba aktarıldı. Sri-Lanka'ya gönderilmesi amaçlanan 20 milyon ABD Doları ise FED sonrası aşamada fon transfer yönlendirme sürecinde aracı Deutsche Bank tarafından tespit edilerek bloke edildi. Bangladeş Merkez Bankası'ndan çalınan 81 milyon ABD Dolarının bir kısmı pesoya çevrildi ve para bir kumarhaneya ait olduğu tespit edilen alıcıya aktarıldı.

Bu örneklerin çoğaldığı bir ortamda Türkiye ise, diğer ülkelerin SWIFT ve benzeri yollar ile sıklıkla karşılaştığı siber saldırılardan korunmak için başta kritik finansal altyapı hizmetlerini barındıran TCMB ve diğer kurumlardaki güvenlik önlemlerini en üst düzeye çıkartıp, tüm sistemlerini güncel ve SOME ekiplerini eğitimli ve hazır halde tutarak uzun döneme yayılan buna benzer hibrit saldırıların önüne geçmek için gereken önlemleri almalı, AB başta olmak üzere tüm paydaşlarla bilgi paylaşımı ve işbirliğini en üst düzeyde tutmalıdır.

Ulaşım & Liman İşletmelerinde Kritik Altyapının Önemi

Ulaşım ve taşımacılık sektörü, hem kritik altyapı operatörlerinin operasyonel yükünü hem de değerli müşteri verilerini barındırarak siber suçlular için iki kat çekici hedefler haline geliyor. 2017'de, Ukrayna'da gerçekleştirilen ve daha sonra bütün ülkelere yayılan NotPetya saldırısında kötü amaçlı yazılım Maersk'in BT sistemlerine sızdı ve küresel nakliye şirketine 300 milyon ABD Doları zarara mal oldu.[39] Maersk'in yaşadığı bu zarara ek olarak, kurumun bütün operasyonel faaliyetleri işlemez hale geldi, sahada yaşanan sorunlar yüzünden kurum müşterilerine karşı marka ve değer kaybı yaşadı.

Benzer bir saldırı senaryosunda, bilgisayar korsanları Colorado'da ABD Colorado Ulaştırma Bakanlığı'na ait 2.000 bilgisayarı kapattı.[40] Ulaşım sektöründe diğer sektörlerden farklı olarak karşılaşılan güvenlik açıklarından biri, sinyalizasyon, sensörler ve teçhizatların bilgi teknolojilerinden farklı olarak operasyonel teknolojileri de bünyesinde barındırmasıdır. Bu tarz sensör bazlı teknolojiler saldırılara karşı hem daha savunmasız hem de manipüle edilmesi daha kolay olduğundan çok daha fazla risk barındırıyorlar. Bugün ulaşım ve taşımacılık sektöründeki paydaşlar operasyonel teknolojilerdeki bu sorunu görerek sistemlerini daha fazla yedeklemek veya daha fazla izlemek zorunda kalıyorlar. Bu, hem altyapı ve donanım yatırımı bakımından daha fazla maliyete katlanılması hem de daha fazla iş yükü anlamına geliyor.

Operasyonel teknolojilerin barındırdığı bir başka risk unsuru insanlar için fiziksel güvenlik riskleriyle sonuçlanabilecek bir bilgisayar korsanlığı tarafından kesintiye uğratılabilirler. Hal böyle olunca

[38] https://cybernews.com/editorial/here-are-the-biggest-digital-heists-of-the-last-decade/
[39] Digital Guardian, Cost of the Malware Infection, https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million,
[40] CPR News, https://www.cpr.org/2018/04/06/cdot-mostly-back-online-after-ransomware-attack/, 06.04.2018

denetlemekle yükümlü kamu kurumları ve düzenleyiciler daha sıkı direktifler ve mevzuatlar yayınlayarak kurumlar üzerinde ekstra baskı uyguluyor.

Benzer şekilde, Avrupa Komisyonu, şirketlerin direktife uymaması durumunda üst düzey yöneticileri sorumlu tutmayı da içeren ağ ve bilgi sistemleri için siber güvenlik kurallarını güncellemek ve güçlendirmek için öneriler yayınladı. Bununla birlikte, fidye yazılımlarındaki patlama devam ettikçe ve nakliye şirketleri internete daha fazla endüstriyel sensör ve cihaz bağladıkça, seyahat ve ulaşım sektörlerine yönelik siber tehditlerin azalması beklenmiyor, aksine tehditlerin artarak çoğalacağı ön görülüyor.

Bu nedenle ulaşım ve taşımacılık sektöründe yer alan paydaşlara mutlaka siber güvenlik yazılımı kullanmaları, personellerini eğiterek bilgi birikimi ve farkındalığı en üst seviyede tutmaları ve tüm ihtimalleri iyi hesaplanmış bir acil durum eylem planı ile potansiyel riskleri tespit etmeleri önerilir. Bu sayede bir ihlalin zararlarını minimuma indirerek operasyonel süreçlerin çalışmalarına kesintisiz olarak devam etmesi hedeflenir.

ABD Tarafından Gerçekleştirilen Çalışmalar

CISA (Cybersecurity and Infrastructure Security Agency)
CISA, Amerika'nın siber savunma ajansı olarak kritik altyapı güvenliğini sağlaması için ulusal koordinatör görevini üstlenmesi amacıyla 16.11.2018 tarihinde kurulmuştur. CISA şu anda ABD'nin siber güvenlik yeteneklerini geliştirme çabalarına öncülük ederken kritik altyapıya yönelik riskleri anlamak, yönetmek ve azaltmak gibi temel görevleri vardır. Bunun yanı sıra, CISA'nın Kongre tarafından atanan iki rolü daha vardır. Birincisi, tüm sektörlerde siber güvenliğin operasyonel liderliğini üstlenmesidir. Ayrıca kritik ABD altyapıları da dahil olmak üzere siber ve fiziksel altyapıya yönelik riski azaltmak için kamu ve özel sektörle birlikte çalışması beklenmektedir. ABD, bu konuda genel olarak kamu için risk barındıran ya da fazla kaynak gerektiren projelerde kamu – özel sektör işbirliği modelinin uygulanmasını tercih ediyor. İşbirliği modellerinin kurulması ve yönetilmesini de kongre tarafından tanımlanan ikinci rol olarak söyleyebiliriz.

Oluşturulan işbirliği modellerinin daha somut çıktılar sağlayabilmesi için 2019 yılında CISA, ABD'nin güvenliği, ekonomisi ve halk sağlığı için kritik öneme sahip olduğunu tespit ettiği hükümet ve özel sektörün 55 kritik işlevini yayınladı. CISA yetkililerine göre, bu yeni çerçeve, kilit sistemlerdeki ve teknolojilerdeki sorunların 16 kritik altyapı sektörü dahilinde nasıl erken tespit edilebileceği yada en az tahribat ile çözümlenebileceğini daha iyi değerlendirmeyi amaçlıyor.

Kritik altyapının korunması ile ilgili oluşturulması önerilen KÖİ çalışmalarını desteklemesi için CISA tarafından yönetilen çeşitli fon ve programlar mevcuttur.

Siber Güvenlik Hibe Programı; CISA tarafından yönetilen 1 milyar ABD doları bütçesi vardır. Çalışma, siber güvenlik planlarının uygulanmasını ve siber güvenlik tehditlerinin ele alınmasını içerir.

Siber Müdahale ve Kurtarma Fonu; CISA tarafından yönetilen 100 milyon ABD Doları fon bütçesine sahip olan SOME yasasının bir çıktısıdır.

Risk Yönetimi Ajansları; CISA tarafından yönetilen 35 milyon ABD Doları risk yönetimi bütçesi vardır. CISA'nın sektörler arası uzmanlığı desteklemek için federal hükümet genelindeki Sektör Risk Yönetimi Ajansları ile koordinasyon sağlamasına yardımcı olacaktır.

Siber güvenlik araştırma fonu; CISA tarafından yönetilen 14.5 milyon ABD doları bütçesi vardır. Akademik veya federal olarak finanse edilen araştırma merkezleri, siber güvenliği güçlendirmek için teknoloji üzerine araştırma ve geliştirmeye uygundur.

12 Eylül 2022 tarihinde, CISA ilk kapsamlı siber güvenlik eylem planı olan "2023–2025 CISA Stratejik Planını" yayınladı".[41] Stratejik planı, ABD'nin karşı karşıya kaldığı siber tehditler ve küresel bir siber alanı kapsayan risk ortamına karşı kurulmuştur. Strateji planı içerisinde 2025 yılına kadar uygulanması planlanan 4 temel amaç yer almaktadır. Sırasıyla; siber savunma, risk yönetimi, operasyonel işbirliği ve iş gücü - yeteneklerin birleştirilmesi olarak kabul edebiliriz.

Beyaz Saray

Beyaz Saray kritik altyapı konusunda oldukça erken aşamada aksiyon almıştır. Bu alanda ilk kamu düzenlemeleri 1996 yılında yayınlanmıştır. İlgili yürütme emri uyarınca kritik altyapıların belirlenmesi, koruma yöntemlerinin tespit edilmesi ve uygulamaya konulması konusunda çalışmak üzere alanında uzman kişilerin yer aldığı bir kritik altyapı koruma komisyonu kurulmuştur. Sorumlu komisyon tarafından telekomünikasyon sektörü bileşenleri, elektrik üretim santralleri, petrol depolama ve taşıma birimleri, bankacılık ve finans merkezleri, toplu taşıma sistemleri, temiz su şebekeleri ve kamunun yaşamsal faaliyetlerine yön veren servisler (sağlık, emniyet ve itfaiye dahil) ilk aşamada belirlenen kritik altyapılar olmuştur. Yapılan bu çalışmanın sonuç raporunda, belirlenen kritik altyapı tesislerinin 5 yıl içerisinde tamamen iç kaynaklarla koruma ve kesintisiz çalışma yetkinliğinin kazanılması hedef olarak belirlenmiştir. Ayrıca, bu rapor ile belirlenen kritik altyapıların korunması konusunda fiziksel yetkinliklerin dışında ilk kez siber yetkinliklerden de faydalanılması ihtiyacı ortaya konmuştur.

Kritik altyapıların korunmasına yönelik yapılan bu çalışmalardan sadece birkaç yıl sonra ABD tarihinin en büyük terör saldırılarından birisi olan 11 Eylül Saldırısı gerçekleşti. Bu terör saldırısından sonra ilk yürürlüğe konan yasanın kapsamı daha da genişletildi. 8 Ekim 2001'de imzalanan yeni yasa ile birlikte ilk kez İç Güvenlik Ofisi kuruldu ve bakanlıklar arasında işbirliği ortamı yaratarak başta kritik altyapının güvenliği olmak üzere koordinasyon sağlama görevi verilmiştir.

Şubat 2013'de yayınlanan yeni bir siber güvenlik yasası ile iki ayrı Ulusal Kritik Altyapı Merkezi oluşturulması kararı alınmıştır. İç Güvenlik Bakanlığı tarafından yönetilecek olan, birisi fiziksel altyapı ve diğeri siber altyapı için iki merkez bulunacaktır. Bu merkezler tarafından öncelikli olarak aşağıdaki başlıklar hedeflenerek çalışmalar yürütülecektir;

1. Güvenli ve dayanıklı altyapı sistemlerini mümkün kılmak için ülke içi ve dışında Ar-Ge'yi teşvik ederek kritik altyapı özelinde geliştirilen siber teknoloji ürünlerinin desteklenmesi.

2. Potansiyel etkileri belirlemek için siber saldırı modelleme yeteneklerinin geliştirilmesi bir olay veya tehdit senaryosunun kritik altyapının üzerindeki etkilerini ölçerek altyapının yedeklenmesi ve potansiyel risklerden doğacak tahribatın minimuma indirilmesinin amaçlanması.

3. Siber Güvenlik Eylem Planı'na bağlı kalarak, planı destekleme çabalarına öncelik verilmesi ve başarıya ulaşması için gereken aksiyonların alınması.

NATO

NATO'nun 4 Nisan 1949 tarihinde imzalanan Washington Antlaşması ile kuruluşundan itibaren, antlaşmanın en kritik ve ön planda olan maddesi hiç şüphesiz 5. maddedir. Bu madde 22 Ekim 1951 tarihinde ittifaka Türkiye ve Yunanistan'ın katıldığı tarihte sadece bir kez revize edilmiş ve o tarihten beri

[41] CISA, 2023 – 2025 CISA Strategic Plan, https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf, 12.09.2022

mevcut haliyle NATO'nun ittifak içerisindeki savunma ve stratejik işbirliği politikalarının şekillenmesinde büyük bir etkiye sahiptir. 5. Madde:

> "*Taraflar, Kuzey Amerika'da veya Avrupa'da içlerinden bir veya daha çoğuna yöneltilecek silahlı bir saldırının hepsine yöneltilmiş bir saldırı olarak değerlendirileceği ve eğer böyle bir saldın olursa BM Yasası'nın 51. Maddesinde tanınan bireysel ya da toplu öz savunma hakkını kullanarak, Kuzey Atlantik bölgesinde güvenliği sağlamak ve korumak için bireysel olarak ve diğerleri ile birlikte, silahlı kuvvet kullanımı da dahil olmak üzere gerekli görülen eylemlerde bulunarak saldırıya uğrayan taraf ya da taraflara yardımcı olacakları konusunda anlaşmışlardır. Böylesi herhangi bir saldın ve bunun sonucu olarak alınan bütün önlemler derhal Güvenlik Konseyi'ne bildirilecektir. Güvenlik Konseyi, uluslararası barış ve güvenliği sağlamak ve korumak için gerekli önlemleri aldığı zaman, bu önlemlere son verilecektir*."[42] hükmünü içermektedir.

NATO, kuruluşundan itibaren on yıllar boyunca 2. Dünya Savaşı'nın etkileri ve Soğuk Savaş çevresinde politikalarını şekillendirdikten sonra, ABD'de 11 Eylül 2001 tarihinde yaşanan terör saldırısı ile birlikte kritik altyapıyı içerecek şekilde bir dizi yeni strateji belirleme konusunda harekete geçmiştir. Günümüze kadar 5. madde sadece bir kez bu saldırı sonrası devreye alınırken, takip eden süreçte ABD'nin başını çektiği müttefik devletler kritik altyapının önemini vurgulayıp, teknolojinin gelişmesi ile birlikte siber uzayında potansiyeli konusunda teoriler geliştirmeye başladılar. NATO'nun siber güvenliğe yaklaşımı, öncelikli olarak teknik terimler ve teori tartışmaları arasında geçerken, kısa sürede ittifakın geleceğe dönük stratejileri için olmazsa olmaz bir nokta olarak fikir birliğine varıldı. Siber yetenekleri güçlendirme ihtiyacı bu bağlamda ilk olarak müttefik liderler tarafından 21 Kasım 2002'de Prag'da yapılan zirve toplantılarında kabul edildi. Zirve sonrası yayınlanan Prag Deklerasyonu'nun 4f maddesi ile ilk kez resmi olarak kendine yer bulmuş oldu.[43]

Estonya'nın kamu ve kritik altyapısı 2007'de siber saldırılarla karşı karşıya kaldıktan sonra NATO, konuyu bir ileri boyuta taşıyarak devletler arasındaki bir çatışmanın siber bir boyut içerebileceğini kabul etti ve 2008'deki Bükreş Zirvesi'nde ilk siber savunma politikasını benimsedi. Bükreş Zirvesi'ni takiben NATO Siber Savunma Gücü (CCDCOE) kuruldu ve aktif faaliyete başladı.

2008 yılından beri NATO bünyesinde teknoloji geliştirme, strateji yönetimi, siber savunma operasyonları ve mevzuatlar olmak üzere dört ana başlıkta disiplinler arası araştırma, eğitim ve tatbikatlar tüm üye ülkelerin katılımı ile gerçekleşmektedir. CCDCOE bünyesinde dünyanın en büyük siber güvenlik tatbikatı Locked Shields dışında, yıllık siber güvenlik konferansı CyCon ve siber operasyonları uluslararası mevzuat yönünden inceleyen Tallinn Kılavuzu gibi önemli projeler de yer alıyor.

05 Eylül 2014 tarihinde gerçekleşen Galler zirvesinde, siber uzayda uluslararası hukukun geçerli olduğu kabul edildi. Böylece, yapılan bir siber saldırının etkisinin müttefikler için geleneksel bir saldırı kadar tehlikeli olabileceğinden, siber güvenliğin NATO'nun 5. maddesine bağlı olarak toplu savunma stratejisinin bir parçası olarak Galler Deklarasyonu'nun 72. ve 73. Maddeleri ile ilan edildi.[44] Siber uzayın da dahil olması ile hibrit savaş kavramı hayatımıza girmiş oldu.

NATO'nun 09 Temmuz 2016'daki Varşova Zirvesi sonrası yayınlanan bildirinin 70. ve 71. maddelerini[45] müteakiben, NATO'nun bir siber operasyonlar doktrini oluşturması ve askeri alanda siber yeteneklerin vakit kaybetmeden geliştirilmesi kararları alındı. Oluşturulan doktrin nihayetinde 29 Ocak 2020 tarihinde

[42] NATO, Collective Defence & Article 5, https://www.nato.int/cps/en/natohq/topics_110496.htm, 20.09.2022
[43] NATO, Prague Summit Declaration, https://www.nato.int/cps/en/natohq/official_texts_19552.htm?,
[44] NATO, Wales Summit Declaration, https://www.nato.int/cps/en/natohq/official_texts_112964.htm, 05.09.2014
[45] NATO, Warsaw Summit Communique, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, 09.07.2016

"NATO Müttefikleri için Siber Uzay Ortak Doktrini" adıyla yayınlandı.[46] Bu doktrin, NATO'nun günümüzdeki mevcut siber savunma stratejilerinin temelini oluşturmaktadır. Ayrıca, savunma ve saldırı amaçlı siber operasyonların kapsamı, siber faaliyetlerin planlanması, risk yönetimi, potansiyel tehditler ve roller kapsamlı olarak tanımlanarak NATO'nun siber güvenlik çerçevesi farklı bir aşamaya geçmiştir.

Doktrinin yayınlanması sonrası NATO'nun sahip olduğu BT altyapısı hızla gelişti. Günümüzde NATO, Brüksel'deki siyasi karargahtan askeri bölgelere kadar 60'tan fazla farklı yeri kapsıyor ve her birinin Brüksel'deki merkez üssü ile entegre çalışan yerel BT servisleri bulunuyor. Son on yılda NATO'nun hedef alındığı siber saldırılarda ciddi artışlar gözlemleniyor ve her geçen gün artmaya devam ediyor. NATO buna karşılık olarak sahip olduğu gelişmiş BT servisleri ve siber savunma sistemleri sayesinde her gün şüpheli olayları izleyip kaydediyor. Tüm saldırılar veya şüpheli faaliyetler otomatik olarak algılanır ve ele alınır. Sadece bu anlık izleme süreci 200 kişilik uzman bir siber ekip tarafından gerçekleştiriliyor ve 60 farklı bölgenin ağ sistemleri günün her saatinde savunuluyor.[47]

NATO'nun 2030 vizyonuna doğru adım adım ilerlerken 29 Haziran 2022 tarihinde yayınlanan "NATO 2022 Stratejik Konsepti"[48] ise mevcut durumu özetliyor ve siber uzay konusunda izlenecek stratejiler konusunda detaylı bilgiler veriyor. Belgede yer alan 8 madde de doğrudan siber güvenlik stratejilerine yer verilerek NATO tarafında siber uzayın korunmasının önemi görülüyor. Otoriter aktörler çıkarlarımıza, değerlerimize ve demokratik yaşam tarzımıza meydan okuyor.

Belgeye göre; müttefik devletler için tehlike oluşturan rejimler, geçmişten günümüze nükleer silahlara ve füze yeteneklerine yatırım yapmaktadır. Günümüzde bu silahlara yatırım yapmanın maliyeti oldukça yüksek ve diğer yandan siber silahlara yatırım yapmanın maliyeti bir o kadar düşük olduğu yeni nesil hibrit taktiklerle müttefik devletlerin güvenliğini hedef alıyorlar. Rusya Federasyonu, NATO müttefiklerinin güvenliğine yönelik açık ara en önemli ve doğrudan tehdit olarak tanımlanmıştır. Ayrıca, Çin Halk Cumhuriyeti de NATO çıkarlarına, güvenliğine ve değerlerine meydan okumaktadır. Rusya ve Çin uyguladıkları hibrit ve siber operasyonlar ile sahip oldukları saldırgan söylem müttefikleri sıklıkla doğrudan hedef alır ve ciddi dezenformasyon yaratabilir. Bunu yaparken çoğunlukla, teknolojik ve endüstriyel sektörler, kritik altyapı ve stratejik operatörler ile tedarik zincirleri ilk hedef alınan noktalar olur.

NATO'nun güçlü duruşu modern bir anlayışa sahiptir. Son yıllarda uzay ile tamamlanan nükleer, konvansiyonel ve füze savunma yeteneklerine ek olarak siber savunma yetenekleri müttefik devletlerin savunulması konusunda en etkili argümanlar haline geldi. Uzay ve siber uzayın güvenli kullanımını ve sınırsız erişimini sürdürmek, mevcut anlayış için kritik öneme sahiptir. Bugün müttefik devletlere siber yöntemlerde dahil olmak üzere yapılacak herhangi bir saldırının NATO'nun 5. maddesini başlatmasına yol açabileceği açıkça belirtilmektedir.

Son yıllarda yapay zeka başta olmak üzere, siber güvenlik, bulut bilişim, kuantum bilgisayarlar, otonom teknolojiler, biyoteknoloji, hipersonik uzay teknolojileri, 5G ve blokzinciri gibi teknolojiler sebebiyle tüm dünyada dinamikler hızla değişiyor. Örneğin Çin Halk Cumhuriyeti, sonraki on yıl içerisinde yapay zeka alanında dünyanın lider gücü olmayı hedefliyor. Savunma gücünü revize edebilmek için NATO'nun yeni stratejilerinin önemli bir noktası olarak, müttefikler tarafından yeni teknolojileri kapsayan DIANA adı

[46] NATO, Allied Joint Doctrine for Cyberspace Operations, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf, 29.01.2020
[47] NATO, Cyber Defence, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf, 21.04.2021
[48] NATO, 2022 Strategic Concept, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf, 29.06.2022

verilen yeni bir inovasyon geliştirme süreci başlatılmıştır.[49] DIANA programı kritik teknolojiler üzerinde kamu, özel sektör ve akademinin işbirliğini artıracak, birlikte çalışabilirliği teşvik edecek ve sivil inovasyondan yararlanarak hızlı bir dönüşüm sağlayacaktır. DIANA, dünyanın her yerindeki NATO ofisleri, BT ekipleri ve test merkezlerini içerecektir. Müttefikler ayrıca bu proje kapsamında çok uluslu ve geniş katılımlı bir fon oluşturma konusunda da anlaştılar.

TÜRKİYE'DE MEVCUT DURUM VE YAPILAN ÇALIŞMALAR

Türkiye, sahip olduğu jeopolitik konumu nedeniyle farklı kurum ya da kişiler tarafından sıklıkla siber saldırıların hedefi olmaktadır. Ulaştırma ve Altyapı Bakanlığı tarafından yapılan açıklamaya göre 2020 yılında 118 bin 470 Siber Saldırı gerçekleşirken, bu sayı 2021'de 84 bin 113'e gerilemiştir.[50] Her 6.24 dakikada bir siber saldırıyla karşı karşıya kalıyor olunması meselenin ciddiyeti hakkında önemli bir işarettir. Nitekim 27 Ekim 2019 tarihinde yaşanan ve telekomünikasyon kurumları ile bankaların kritik altyapısını hedef alan siber saldırı sonucunda başta Türk Telekom ve Garanti Bankası olmak üzere pek çok büyük kurumun operasyonel süreçleri durma noktasına gelmiş ve web sitelerine bir süreliğine erişim sağlanamamıştır.[51] Ayrıca Türkiye'deki kamu kurumlarının günde ortalama 82 siber saldırıyla karşı karşıya kaldığını da dikkate almak gerekir.[52]

Yapılan yatırımlar ve gelişen altyapı sayesinde her yıl düzenli olarak yapılan Global Siber Güvenlik İndeksi çalışmasında da Türkiye yakaladığı ivme ile 11. Sıraya kadar yükselmiştir.[53]

Regülasyon ve Kamusal Düzenlemeler

Kritik altyapı kavramının ortaya çıkması ile birlikte Türkiye'de bu alanda sırasıyla pek çok adım atmıştır.

İlk olarak Kasım 2008'de yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu (EHK)[54], ile birlikte kritik altyapı konusu resmi olarak Türkiye'nin gündemine girmiştir. Yürürlüğe giren yasa ile birlikte kritik altyapılarla ilgili sektörler, kurumlar, konumlar ve sahip oldukları riskler belirlenerek, siber güvenlik merkezlerinin kurulması, denetlenmesi, gerekli müdahalelerin gerçekleştirilmesi ve sorumlu kişi ve kuruluşlara eğitimler verilerek ülkenin kritik altyapısının kontrol altında tutulması hedefi ortaya konmuştur.

Bu çalışma sonrasında ise, tespit edilen kritik altyapılar ile bunlara bağlı kurum ve kuruluşlarının korunması için Eylül 2011 tarihinde EHK'ya bağlı olarak; ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordine edilmesi amacıyla Ulusal Siber Olaylara Müdahale Merkezi ile buraya bağlı olacak şekilde çok sayıda Siber Olaylara Müdahale Ekibi'nin kurulması ve faaliyete geçmesi kararı alınmıştır.

Ulusal anlamda bir strateji ve eylem planının ortaya konması ise 2 yıl gibi bir süre almıştır. 2011 yılındaki karar sonrasında Kurul kısa süre içerisinde ulusal siber güvenlik eylem planının geliştirilmesi için

[49] NATO, DIANA, https://www.nato.int/cps/en/natohq/news_194587.htm , 07.04.2022
[50] Daily Sabah, Cyber Attacks Targeting Türkiye Dropped in 2021, https://www.dailysabah.com/Türkiye/cyberattacks-targeting-Türkiye-dropped-in-2021/news, 27.02.2022
[51] TRT News, Türkiye'ye yönelik Siber Saldırılar Bertaraf Edildi, https://www.trthaber.com/haber/turkiye/turkiyeye-yonelik-siber-saldirilar-bertaraf-edildi-437841.html, 28.10.2019
[52] Kadir Has Üniversitesi, https://panorama.khas.edu.tr/kamu-kurumlari-gunde-yaklasik-olarak-82-siber-saldiriya-ugruyor-261
[53] Global Cyber Security Index, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf, p:25
[54] Ulaştırma ve Altyapı Bakanlığı, Elektronik Haberleşme Kanunu, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/5809-ehb.pdf

çalışmalara başlamış ve ilkini 2013-2014 yılları, ikincisini 2016-2019 yılları ve sonuncusunu ise 2020-2023 yılları için güncelleyerek faaliyete alınmıştır.

2020 – 2023 yılları arasında duyurulan Siber Güvenlik Eylem Planı, kritik altyapıyı birinci öncelik olarak belirlemiştir. Eylem Planının:

Misyon bölümünde; "Siber güvenliğin milli güvenliğimizin ayrılmaz bir parçası olduğu bilinci ile kritik altyapılarımız başta olmak üzere siber uzaydaki varlıklarımızın tehditlerden korunmasına ve siber olayların muhtemel etkilerini azaltmaya yönelik çalışmaları ilgili tüm paydaşlarla koordineli olarak gerçekleştirmek", tarifiyle kritik altyapının eylem planının temelini oluşturduğu anlaşılmaktadır.

Eylem Planı maddeleri açısından ise 3 farklı referans ile da kritik altyapı hedef olarak belirlenirken, Kritik Altyapının Korunması ve Mukavemetin Arttırılması stratejik amacı ile tam 22 eylem planı maddesi ilişkilendirilmiştir;

- Kritik altyapılarımızın siber güvenliğinin 7/24 korunması.
- Kritik altyapı sektörlerinde düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi.
- Kritik altyapı sektörlerinde, BT ürünlerinde üretici bağımlılığının önüne geçilmesi.

İş Birlikleri & İlgili Kurumlar

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
Gelişen teknolojiler, toplumsal talepler ve kamu sektöründeki reform eğilimleri doğrultusunda, farklı kurumlar altında ayrı ayrı sürdürülen dijital dönüşüm, siber güvenlik, büyük veri ve yapay zekâ ile ilgili çalışmaların tek çatı altında toplanması amacıyla, 10 Temmuz 2018 tarihinde 30474 sayılı Resmi Gazete'de T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi kurulmuştur.

Dijital Dönüşüm Ofisi'nin başlıca görevi belirlenen politikalar kapsamında kamu kurumları ve kritik altyapılara yönelik siber güvenlik stratejileri geliştirmek ve uygulanması konusunda paydaşlara destek sağlamaktır.

Ofis, kritik altyapıya uygun stratejileri geliştirirken öncelikle KÖİ modeline uygun olacak şekilde özel sektörün kapasitesinin kritik alanlara yönlendirilmesi ve maksimum verim alınacak şekilde kullanılabilmesi yer alır. Her başarılı uygulama kritik altyapı alanlarında yerli ve milli siber güvenlik ürünlerinin geliştirilmesi ile sağlanır. DDO ayrıca, başarılı olarak üretilen yerli ve milli ürünlerin satışı konusunda tanıtımlara katkıda bulunur, ihracat konusunda destek sağlar ve çözümlerin kullanımının kamuda yaygınlaştırılmasına yönelik yurt içinde çeşitli çalışmalar yapar.

Ofis, siber güvenlik alanında farkındalığın arttırılması ve eğitim programlarının oluşturulması konusunda da güçlü destek sağlar. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Yükseköğretim Kurulu arasında bu amaçla, siber güvenlik meslek yüksekokullarının açılmasına ilişkin protokol 05 Ekim 2022 tarihinde imzalanmıştır. İmzalanan bu protokol ile siber güvenlik alanında yetkin ve nitelikli iş gücü inşa edilmesini, siber güvenlik öğretim programlarının geliştirilmesini, alandaki eğiticilerin beceri ve yetkinliklerinin artırılmasını, yükseköğretimde mevcut siber güvenlik eğitim içeriklerinin zenginleştirilmesini, siber güvenlik öğretim programlarının yaygınlaştırılmasını ve siber güvenlik alanındaki istihdamın artırılmasını amaçlanmaktadır.[55]

[55] Yüksek Öğretim Kurulu, Siber Güvenlik Meslek Yüksek Okulları Açılıyor, https://www.yok.gov.tr/Sayfalar/Haberler/2022/siber-guvenlik-meslek-yuksekokullari-aciliyor.aspx, 05.10.2022

DDO altında çalışmalarını sürdüren bir başka paydaş Türkiye Siber Güvenlik Kümelenmesi Platformu'dur. Pazara erişim, inovasyon, yeteneğe erişim, etkileşim ve teknolojik üstünlük olmak üzere 5 ana başlıkta faaliyetlerini yürütmektedir. Platformun ana hedefleri arasında Türkiye'deki siber güvenlik firmalarının sayısını artırmak, üyelerinin teknik, idari ve finansal açılardan gelişimine destek olmak, siber güvenlik ekosisteminin standartlarını geliştirmek, üye firmaların ulusal ve global pazarda rekabet gücünü artırmak bulunuyor. Siber kümelenme ekosisteminde 38 farklı üniversiteden 42 farklı ekip yer alıyor.

TÜBİTAK

Tübitak, Türkiye'nin siber güvenlik alanında kritik altyapı savunucularına her alanda destek sağlamaktadır. BİLGEM bünyesinde yer alan Siber Güvenlik Enstitüsü (SGE) bu alanda ana üstlenici konumundadır. Özellikle son yıllarda yaptığı çıkışlarla adıdan ciddi anlamda söz ettiren kurum organizasyon yapısını ve hedeflerini her geçen gün genişletmektedir.

TSK liderliği ve SGE İleri Siber Güvenlik Araştırmaları Enstitü Müdür Yardımcılığı Birimi'nin katılımıyla, siber savunma alanında işbirliğinin arttırılmasına yönelik bir siber savaş tatbikatı olan 2022 yılındaki NATO Kilitli Kalkan Tatbikatı'ndaki simülasyonunda Türkiye, 9'uncu olarak tamamlamıştır.[56] 10 kişilik alanında uzman ekip çok sayıda farklı siber saldırıyı etkisiz hale getirmeyi başarmıştır.

SGE, bir yandan da girişimleri bu alana teşvik etmek için Ar-Ge konularında kurumlara farklı başlıklarda destek sağlamaktadır. Bu kapsamda, girişimlere teknolojide yenilikler ve sektörde ihtiyaç duyulan nitelikler aktarılarak uygun olabilecek iş modellerini sunmaya yönelik çalışmalar gerçekleştilmektedir. Kamu ve özel işbirliği çalışmalarında, BILGEM bünyesinde yer alan Teknoloji Transfer Ofisinin imkanlarından ve tecrübelerinden faydalanılmaktadır. Özellikle Ar-Ge projelerinin ürüne dönüşme aşamalarında özel sektörün sahip olduğu personel ve bilgi kaynağı önemli bir avantaj olarak görülmektedir.

Siber güvenlik alanında bilgi paylaşımı var olan sistemlerin daha etkin hale gelmesinde önemli bir faktördür. Bu amaçla özellikle siber tehdit oluşturan etkenler, saldırı imzaları, zararlı yazılım veritabanları gibi verilerin özel sektör ile paylaşılmasına, benzer şekilde özel sektör tarafından elde edilen bilgilerin de SGE tarafından değerlendirilmesine önem verilmektedir. Bu amaçlı karşılıklı bilgi paylaşımına imkan veren gizlilik anlaşmaları ve protokoller imzalanmaktadır.

Kamu - Özel İş Birliği kapsamında yapılan ortak çalışma başlıkları aşağıdaki gibidir;

- Başta TUBITAK olmak üzere siber güvenlik alanında Ar-Ge çalışmaları için fon sağlayan yerli ve yabancı kuruluşlarla ortak projeler geliştirmek için uygun ortamı yaratmak ve girişimlerin sağlanan fonlardan en etkin şekilde yararlanmasını sağlamak.
- Kurumlara özel gerçekleştirilen siber güvenlik projelerinde yerli ürünlere yer vermek.
- SGE özellikle implementasyon, bakım, destek, lisanslandırma ve girişimlerin yer aldığı ticari proje fırsatlarından net çizgilerle uzak durmaktadır. Aynı zamanda girişimler arasında eşit rekabet koşullarının sağlanması için ortaya çıkan fırsatları ilgili tüm girişimlerle paylaşmaktadır.
- Siber güvenlik alanında katma değer sağlayan yada kurumların güvenliğini garanti altına alacak her türlü verinin açık veri prensiplerine dayalı olarak talep edenlerle paylaşımını sağlamak.

Ayrıca, SGE başta risk analizi, sızma testleri, zaafiyet testleri, zararlı yazılım analizi ve sertifikasyon standartlarının sağlanması olmak üzere pek çok alanda kamu ve özel kurumlara danışmanlık hizmeti sağlamaktadır.

[56] NATO, Cyber Coalition, https://www.act.nato.int/cyber-coalition

Bilgi Teknolojileri ve İletişim Kurumu (BTK)

Bilgi Teknolojileri ve İletişim Kurumu; 5809 nolu Elektronik Haberleşme Kanunu'nun 05 Kasım 2008 tarihinde resmi gazetede yürürlüğe girmesi sonrasında.[57] Türkiye'nin siber güvenlik ile kritik altyapının korunması konusunda en önemli kurumu haline gelmiştir. Yürürlüğe giren EHK'yı takiben ulusal siber güvenlik eylem planlarının hazırlanması, sorumlu savunma birimlerinin oluşturulması, mevzuatların geliştirilmesi, kamu ve özel sektör arasında işbirliği fırsatlarının teşvik edilmesi, farkındalık yaratılması gibi pek çok sorumluluk BTK bünyesinde toplandı.

Ayrıca, son yıllarda yürürlüğe alınan 2016/28 sayılı 'Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi[58], genelgesi ile kamu kurumlarının çevrimiçi ortam üzerinden ortak çalışma prensibini benimsemesi amacı ortaya konmuştur. Bu amaca uygun olarak, kamu kurum ve kuruluşları arasında güvenli haberleşme ve veri paylaşımı Türk Telekom gibi bazı paydaşlarında yer aldığı grup ile birlikte BTK bünyesinde toplanmıştır. Genelge ile bunlara ek olarak, kurumlar arası iletişimde mevzuatlara uygun standartların sağlanması, ortak uygulamalar için uygun altyapının oluşturulması, planlanan kamu çevrimiçi ağı için veri merkezlerinin kurulması ve siber saldırılara karşı güvenliğinin sağlanması gibi sorumluluklarda da yine BTK ana üstlenici rolünü üstlenmiştir.[59]

Bunlara ek olarak ülkemizde yaşanan siber saldırıları ve potansiyel risklerin boyutunu göz önünde bulundurularak BTK bünyesinde 27/05/2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi kurulmuştur. USOM bünyesinde 4 ana faaliyet alanı olup bunların en başında "kritik altyapıların korunması" başlığı bulunmaktadır.[60] Ayrıca kritik altyapıların korunması amacıyla, kritik kamu kurumları ve kritik altyapılar olmak üzere kamunun kaynaklarına ilişkin zafiyet taraması veya hizmet sürekliliğinin sağlanmasına yönelik izleme faaliyetleri buna paralel olarak "Kasırga Projesi" ile sürdürülmektedir. Bu faaliyetlere ek olarak proje bünyesinde kamunun kritik altyapılarını barındıran, toplamda 16 milyon IP adresi için periyodik olarak zafiyet ve risk taraması yapılarak kontrol altında tutulmaktadır. Türkiye'de elektronik haberleşme, finans, enerji, su yönetimi, ulaşım ve kritik kamu hizmetlerinin kritik sektörler olarak belirlendiğine işaret eden Evren, bu kapsamda 14 sektörel SOME, 2077 kurumsal SOME'nin faaliyet gösterdiğini kaydetti. Evren, SOME'lerde 6264 siber güvenlik uzmanının ise ulusal siber güvenliğin sağlanması yönünde çalışmalarını sürdürdüğüne dikkati çekti.[61]

Ayrıca; farkındalığın arttırılması, ekosistemin geliştirilmesi gibi amaçlar için geniş ölçekli konferanslar[62] ve çok sayıda SOME'nin katılımıyla siber güvenlik tatbikatları BTK tarafından gerçekleştirilmektedir.[63]

BTK içerisinde faaliyet gösteren kuruluşlardan bir diğeri Siber Güvenlik İnisiyatifi'dir. Sektör paydaşlarının katılım sağladığı ve hedefi siber güvenlik alanında çalışmalar yaparak, tüm paydaşların görüşlerini toplayıp, kurumlar arasında fikir alışverişi ve işbirliğini sağlamaktır.

---

[57] HGM, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/5809.pdf, 05.11.2008
[58] HGM, 2016/28 KamuNet Genelgesi, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/kamunetgenelgesi.pdf
[59] Resmi Gazete, KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usül ve Esaslar Hakkında Tebliğ, Bölüm:2 Madde:4, 21.06.2017
[60] BTK, USOM & Kurumsal Siber Olaylara Müdahale Ekibi, https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, 15.12.2017
[61] Anadolu Ajansı, Siber Güvenlik Ulusal & Uluslararası Güvenlik Stratejilerinde Yerini Aldı, https://www.aa.com.tr/tr/ekonomi/gokhan-evren-siber-guvenlik-ulusal-ve-uluslararasi-guvenlik-stratejilerinde-yerini-aldi/2599110, 27.05.2022
[62] Türkiye Bilişim Derneği, 5. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi, https://www.siberguvenlikzirvesi.org.tr/2022/, 25.03.2022
[63] USOM, Finans Sektörü Siber Kalkan 2022 Tatbikatı, https://www.usom.gov.tr/duyurular/finans-sektoru-siber-kalkan-2022-tatbikati, 21.10.2022

Siber Güvenlik İnisiyatifi'nin bunun dışında farklı görevleri de vardır. KOBİ'lere siber güvenlik konusunda farkındalık eğitimleri vermek, toplumsal farkındalık oluşturmak, koruma tedbirlerini oluşturmak ve kılavuzlar yayınlamak olarak sıralanabilir.[64]

Siber Güvenlik İnisiyatifi kapsamında bazı çalışma grupları oluşturulmuştur. Söz konusu gruplar aşağıdaki gibidir;

- Farkındalık, Eğitim ve Rapor Çalışma Grubu
- Siber Olaylarla İlgili Mevzuat ve Koordinasyon Çalışma Grubu
- Ulusal Siber Olaylara Müdahale Organizasyonu Çalışma Grubu
- Teknik Araştırmalar ve Standartlar Çalışma Grubu
- Siber Tehditler ile Mücadele Çalışma Grubu

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) & Serbest Piyasası Kurulu (SPK)
Türkiye'de finans alanındaki standartların oluşturulup uygulanması, denetlenmesi ve kontrol altında tutulmasından sorumlu kurum SPK ve BDDK'dır. Bu alanda yapılan ve resmi gazetede yayınlanan 15 Mart 2020 tarihli son düzenleme[65] ile bankaların bilgi sistemleri ile elektronik bankacılık alanında finansal ve kritik altyapıların korunması konusunda kurumların alması gereken önlemler, görevler ve sorumluluklar detaylı şekilde ortaya konmuştur. Düzenleme ile bugünün ve geleceğin bankacılık anlayışını ortaya koyan dijital bankacılık, uzaktan kimlik ve hesap yönetimi, mobil bankacılık gibi uygulamaların kritik altyapılarını ön planda tutan güvenlik ihtiyaçları ve gereksinimler geniş bir çerçeveye yerleşmiş ve sınırları net olarak ortaya konmuştur. Bu kapsamda SPK ve BDDK, ilgili finansal kuruluşları asli sorumlu olarak belirlemiş ve kişisel verilerin güvenliği, sistemlerin kesintisiz ve güvenli çalışabilmesi, yaşanacak herhangi bir sorunda vatandaşların mağdur edilmemesi ve mağdur olunması durumunda yaşanan maddi manevi zararlardan sorumlu olarak, kritik altyapısını ilgili tebliğler uyarınca korumakla yükümlü olan finans kuruluşları olarak teyit edilmiştir. Siber Güvenlik Stratejisi'nde yer alan maddeler uyarınca ISO 27001 sertifikası alınmasının önemi ve rolü, penetrasyon kontrollerinin düzenli ve standart hale getirilmesi, sistem odaları, sunucular ve ağ sistemlerinde bulunması gereken asgari güvenlik önlemlerinin altı çizilerek önemine vurgu yapılmıştır.

Uluslararası Kuruluşlarla Yapılan İşbirliği Çalışmaları
AB Siber Güvenlik İş Birliği Organizasyonu, kurulduğu günden bu yana 28 farklı ülkede 160 organizasyon ile çok sayıda işbirliği projesi geliştirilmesini sağlamış ve çalışmalarını aralıksız sürdürmektedir. Türkiye, 2 farklı yerel organizasyon ile AB ülkelerinden kurulumların da katılımıyla 2 siber güvenlik projesini bugüne kadar ECSO sayesinde tamamlamıştır.[66]

NATO Siber Savunma Mükemmeliyet Merkezi, NATO'nun siber savunma kapasitesinin artırımı amacıyla Estonya'nın başkenti Tallinn'de kurulmuş uluslararası bir askeri merkezdir. Merkez; siber güvenliğin gerek teknik, gerek hukuki ve uluslararası ilişkileri ilgilendiren konularında çok çeşitli faaliyetler yürütmektedir. Türkiye, Siber Savunma Mükemmeliyet Merkezi ile birlikte ortak tatbikatlar düzenlemekte ve siber savunma gücünün NATO nezdinde gelişmesi için ortak çalışmalarını sürdürmektedir.

[64] BTK, Siber Güvenlik İnsiyatifi, https://www.btk.gov.tr/siber-guvenlik-inisiyatifi, 15.12.2017
[65] Türkiye Official Newspaper, https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm, 15.03.2020
[66] ENISA, Market Study of NIS Product & Services, https://www.enisa.europa.eu/events/enisa-validation-workshop-market-study-of-nis-products-and-services/3TheDSMandcPPPinitiativeLuigiRebuffi.pdf

Kurulduğu günden bu yana AB ile yakın ilişkiler içinde olan TÜBİTAK SGE, Siber Savunma Tatbikatları gibi uzmanlık alanına giren teknik konularda kuruluş ile ortak çalışmalar yürütmeye başlamıştır. İlerleyen vadede bu işbirliklerinin artırılarak devam ettirilmesi hedeflenmektedir.

SGE ülkemizin NATO nezdinde toplantı, tatbikat ve projelerde temsili ile siber güvenlik güncel konulara hakim olunması, teknolojik gelişmelerden haberdar olunması, yetenek, proje ve ürünlerimizin tanıtılmasını ve sunulması amaçlarıyla NATO bünyesinde faaliyet gösteren çalışma gruplarına ve panellere, farklı ülkelerden uzmanlarla beraber, katılım sağlamaktadır.

FIRST, Küresel Olay Müdahale ve Güvenlik Ekipleri Forumu'dur. Bu alanda önde gelen kuruluşlardan birisi ve olay müdahalesi konusunda bir Dünya lideridir. Kuruluş; hükümet, ticari ve eğitim kuruluşlarından çeşitli bilgisayar güvenliği olay müdahale ekiplerini bir araya getirir. Olaylara hızlı tepki vermeyi ve üyeler arasında bilgi paylaşımını teşvik ederek siber saldırıları en hızlı şekilde önlemeyi hedeflemektedir. Türkiye, forum içerisinde 3 farklı ekip ile aktif olarak çalışmalara katılmaktadır. TR-CERT, Turkcell CDC ve Yapı Kredi Bankası CERT ekipleri ile ortak çalışmalar yürütülmektedir.[67]

NATO MISP Zararlı yazılımlar konusunda bilgi birikimine sahip üyelerin bir araya gelerek oluşturduğu bir topluluktur. Bilgi paylaşımı sayesinde, zararlı yazılımların tespit edilmesinin hızlandırılmasını, özellikle antivirusler tarafından tanınmayan örnekler için savunma metotlarının geliştirilmesini ve hedefli saldırılarla baş edilmesi için gereken yöntemlerin ortaya çıkarılmasını hedefler. Üyelerin katkılarıyla içinde arama yapılabilen ve çok yönlü bilgi paylaşımına olanak sağlayan büyük bir veri havuz oluşmuştur. Siber Güvenlik Enstitüsü, özellikle ülkemizi tehdit eden zararlı yazılımların tespit edilmesi, aktivitelerinin izlenmesi ve gerekli önlemlerin alınması hedefleri doğrultusunda NATO MISP topluluğuna aktif katkı sağlamaktadır.

DEĞERLENDİRME & ÖNERİLER

Önümüzdeki 5 yıl içerisinde 5G, blokzinciri, kuantum bilgisayarlar, bulut sistemler ve IOT cihazların daha da yaygınlaşması ile birlikte kritik altyapı barındıran tüm sektörler uçtan uca bilgi teknolojileri ile entegre hale gelecektir. Bugüne göre çok daha fazla veri üretilecektir. Bu daha yüksek veri hacmini yönetmek için çok daha yüksek kapasiteli güç, enerji, altyapı, güvenlik ve eğitim ihtiyacı doğuracaktır. Tahminlere göre sürecin olgunlaşması sonrası, 80 milyar cihaz internet bağlantısına sahip olacak ve günlük hayatımıza dahil olacaktır.[68] Bu dünyadaki her kişi başına ortalama 10 çevrimiçi cihaz anlamına gelmektedir. Bununla birlikte üretilen veri kontrolsüz bir şekilde günden güne büyümeye devam edecek ve mevcut veri dünyası her 2 yılda bir 2 katına çıkarak hızla gelişecektir. Ulaşım sektöründe otonom araçlar, endüstride nesnelerin interneti, telekominikasyonda 5G, finansta blokzinciri başta olmak üzere yeni teknolojilerin sektörler üzerinde büyük etkisi olacaktır.

COVID-19 salgını ile beraber vatandaşların dijital kimliklere sahip olmaları, çevrimiçi alışveriş ve ödeme sistemlerini daha ağırlıkla kullanmaları bilgi işlem gücü ile depolama kapasitesi ihtiyacını hızla artırmak suretiyle daha güçlü sunucu sistemleri ile bulut bilişimi ön plana çıkardı. Tetiklenen otomasyon ile entegrasyon süreci, ciddi bir iş yükü ve bilgi birikimi ihtiyacını da beraberinde getirdiği için operasyonel süreçlerde yapay zeka görevi devraldı.

[67] FIRST, https://www.first.org/members/map#country%3ATR
[68] ENISA, Analysis of the European R&D Priorities in Cybersecurity, https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity, p:8, 01.12.2018

Bu ortamda hükümetler teknoloji devlerinin artan etkisine karşı yasal düzenleme ve müeyyideler geliştirimeye çalıştılar. Ayrıca teknolojide dışa bağımlılığın azaltılması ve teknolojinin yerelleştirilmesi de daha da önemli bir hedef haline geldi. Nitekim yeterli olmasa da aşağıda[69] 2020 yılına ait örneklerden de görüleceği gibi son yıllarda devletler GSYİH içerisinde Ar-Ge paylarını arttırmaya tam da bu nedenle öncelik vermeye başladılar.

- İsrail: Ar-Ge Payı: %5.44 – Bir Önceki Yıla Göre Artış Oranı: %6

  Güney Kore: Ar-Ge Payı: %4.81 – Bir Önceki Yıla Göre Artış Oranı: %4
- ABD: Ar-Ge Payı: %3.45 – Bir Önceki Yıla Göre Artış Oranı: %8.5
- Japonya: Ar-Ge Payı: %3.27 – Bir Önceki Yıla Göre Artış Oranı: %2
- Finlandiya: Ar-Ge Payı: %2.91 – Bir Önceki Yıla Göre Artış Oranı: %4
- Fransa: Ar-Ge Payı: %2.35 – Bir Önceki Yıla Göre Artış Oranı: %7.5
- Norveç: Ar-Ge Payı: %2.28 – Bir Önceki Yıla Göre Artış Oranı: %6
- Estonya: Ar-Ge Payı: %1.75 – Bir Önceki Yıla Göre Artış Oranı: %7.4
- Yunanistan: Ar-Ge Payı: %1.51 – Bir Önceki Yıla Göre Artış Oranı: %18
- Polonya: Ar-Ge Payı: %1.39 – Bir Önceki Yıla Göre Artış Oranı: %5.4
- Türkiye: Ar-Ge Payı: %1.09 – Bir Önceki Yıla Göre Artış Oranı: %1.9

Ulusların gelişen teknoloji ile doğru orantılı olarak siber yetkinliklerini güçlü tutabilmeleri için üzerinde durması gereken noktalar sırasıyla;

- Güvenlik ve gizlilik amacıyla oluşturulan sistemlerin kamu düzeyinde eğitimlerinin verilerek tanıtılması, kullanıcı bilgi birikimi ve deneyiminin arttırılması,
- Tüm bilgisayar bilimi eğitim programlarında güvenlik ilkelerinin öğretilmesini kolaylaştırılması,
- Yeni nesil yazılım mühendislerinin güvenlik prensiplerine sahip olacakları şekilde ilgili eğitimlerin müfredatlara eklenmesi,
- Yapay zekanın siber güvenlik hedefine paralel şekilde kullanımının yaygınlaştırılması, kuantum ve süper bilgisayarlar ile birlikte kriptografi ve bunların algoritmik uygulamaları üzerine araştırma ve yeni teknoloji ürünlerinin üretilmesinin teşvik edilmesi,
- Dağıtık, kompleks birbirine bağlı sistemlerin etki değerlendirmesi için yeni bir yaklaşımın geliştirilmesi,
- Kritik altyapılar arasında entegrasyon ve veri paylaşımını sağlayarak güvenli, birlikte çalışabilir sistemlerin ortaya konması sağlanmalıdır.

Kamu yada özel sektör farketmeksizin, günümüz gereksinimlerine uygun yukarıda maddeler ile sıralanan yatırımları ve atılımları yapmakta geç kalan kritik bir altyapı kuruluşu tehlikeye düşerse, altyapısına bağlı olan tüm kurum ve kuruluşlara sağladığı hizmet devre dışı kalabilir ve saniyede milyonlarca dolarlık kayba neden olabilir. Bu kayıp, veri ihlali, hizmetin kesintiye uğraması, fiziksel yıkım, enerji ve ham madde tedarikinin sağlanamaması gibi farklı sebeplerden kaynaklanabilir.

Öte yandan bu alanda yapılan yatırım ve harcamalara bakmak gerekirse; Kritik Altyapıyı korumak için yapılan harcamaların büyüklüğü 2021'de 133.3 milyar ABD Doları civarında seyrederken, önümüzdeki 5

[69] OECD, Gross Domestic Spending on R&D, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

yıl içerisinde ortalama %3.3 yıllık büyüme oranı ile 2026'ya kadar 157.1 milyar ABD Doları seviyesine gelmesi bekleniyor.[70]

Bu harcamaların en büyük payını bugün olduğu gibi gelecekte de veri ihlallerini önleme girişimleri oluşturacak. veri ihlalleri sayesinde sağlanan verilerin kötü amaçlı kullanımları (sahtekarlık, kurumsal ağ sistemlerine sızma gibi) bir siber saldırının yarattığı tahribat çok yüksek olabilir.

IBM Veri İhlalinin Maliyeti 2022 raporuna göre; 2022'de küresel olarak bir veri ihlalinin toplam ortalama maliyetinin yıllık %2,6 artışla 4.35 milyon dolar olduğunu gösteriyor. Bu rakam, kritik altyapı kaynaklı ihlaller için ortalama 4.82 Milyon ABD Doları olurken, diğer kuruluşlar için ortalama 3.83 Milyon ABD Doları seviyesindedir. Buna göre kritik altyapı kaynaklı ihlaller ortalama olarak diğer herhangi bir ihlale göre %22.9 daha fazla zarara yol açmaktadır.[71]

Kritik altyapıyı korumak için yapılan harcamalarda veri ihlallerinin engellenmesi amacının yanısıra, hükümet düzenlemelerine uyum, saldırıların fiziksel sistemleri etkilemesinin engellenmesi ve endüstri 4.0 ile birlikte OT ağlarını güvenli hale getirme ihtiyacının artması yer alıyor. Bunlara ek olarak, blokzinciri gibi yeni nesil güvenilir teknolojilerin altyapılarda kullanılmak amacıyla geliştirilmesi ve Türkiye gibi geniş coğrafyaya sahip ülkelerde kırsal bölgelerde kablosuz geniş bant kullanılabilirliğinin arttırılması, kritik altyapıyı korumak için yapılacak yatırımlar konusunda sektör paydaşları için yeni fırsatlar oluşturabilir.

Kritik altyapı konusunda olası siber saldırıların etkisini minimuma indirebileceğiniz bir diğer alternatif "sıfır güven yaklaşımı" uygulanmasıdır. Günümüzde, "sıfır güven" düzenine sahip olan kritik altyapı kuruluşları, sıfır güven yaklaşımına sahip olmayanlara göre ortalama 1.17 Milyon ABD Doları daha az etkilenmektedir.[72]

Tüm bu ekonomik fırsatların ve proaktif ortamın gücünden yararlanarak güvenilir bir siber alan yaratmak için siber risklere karşı ağırlıklı olarak Kamu-Özel İşbirliği olarak adlandırılabilecek modeller de ön plana çıkmaktadır. Bunun da temel nedeni siber saldırıların hedefinde olan birçok kritik altyapının aslında özel sektör tarafından kurulması veya işletilmesidir. Söz konusu şebekeler konusunda bilgi birikimi çoğu zaman daha ağırlıklı olarak özel sektörde bulunmaktadır. Dolayısıyla ulusal güvenliğin korunmasından sorumlu olan kamu kesimi ile bu altyapıların sorumluluğunu taşıyan özel sektör arasında etkin bir işbirliğinin tesis edilmesi siber risklerin azaltılması açısından elzemdir. Ayrıca bu modelin başka avantajları da bulunmaktadır. Öncelikle sınırlı kaynakların daha verimli kullanılmasını sağlamakta ve düplikasyonu önlemektedir.

Siber güvenlik alanında KÖİ modelinin tercih edilmesinin bir diğer nedeni de bilgi ve veri paylaşımının gerekliliğidir. Acil durum eylem planlarının sağlıklı şekilde uygulanabilmesi, saldırıların kamu hayatı ve insan sağlığı üzerinde oluşturacağı tahribatı en aza indirebilmek için sektörler ile paydaşlar arası bilgi paylaşımı kritik önem taşımaktadır. Erken uyarı sistemlerinin kullanılabilirliği veya olası saldırı durumlarında kamunun farkındalığı, kaos senaryolarının önlenmesi veya en az hasarla atlatılabilmesi için kritiktir.

Anılan KÖİ modellerindeki hassas bir başarı faktörü kurumsal işbirliğinin etkin denetimidir. Kritik bilgi altyapısına dair risk analizi ve süreklilik planı, altyapı sahiplerinin sorumluluğundadır. Ancak bu faaliyetlerin uygulanması kamu tarafından denetlenmeli ve yönlendirilmelidir. Denetleme ve iyileştirme

[70] Markets & Markets, Market Research Report – Critical Infrastructure, https://www.marketsandmarkets.com/Market-Reports/critical-infrastructure-protection-cip-market-988.html?utm_source=globenewswire&utm_medium=Referral&utm_campaign=paidpr, 01.06.2021
[71] IBM Data Breach Report 2022, The average cost of a data breach in critical infrastructure organizations https://www.ibm.com/downloads/cas/3R8N1DZJ, p:37, 27.07.2022
[72] IBM, Data Breach Costs Reach All Time High, https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High, 27.07.2022

süreçleri ise uzun soluklu işbirliği ve koordinasyon gerektirir. Örneğin Finlandiya'da bu amaç ile kurulan 'Ulusal Acil Güvenlik Ajansı' (NESA), başta siber güvenlik olmak üzere işbirliği fırsatlarının planlanması, analizi, geliştirilmesi ve denetlenmesi için stratejik bir rol üstlenmiştir. Anılan kurum ekonominin kritik sektörlerindeki kilit paydaşları Güvenlik açıklarını değerlendirmekte ve performans analizlerini yapmaktadır. Halihazırda öncülüğünü yaptığı çalışma gruplarında kritik sektörlerde yeralan 1000'den fazla KOBİ ile işbirliği faaliyetlerine devam etmektedir.[73]

Etkili bir KÖİ modeli ulusal siber güvenlik stratejisi ile senkronize politikalar izleyerek, sürdürülebilir risk ve kriz yönetimi süreçlerini kritik altyapı güvenliğini koruma çalışmalarının merkezine konumlandırmalıdır. KÖİ modeli kritik altyapının hangi sektörü için uygulanırsa uygulansın, işbirliğine dahil olan paydaşlar bu kavramlara aşina olmalı ve bunları kendi sektörlerinde ve yetkinlik alanlarında tutarlı bir şekilde sürdürebilmelidir. Söz konusu risk değerlendirmesi olduğunda; riskin azaltılması, risklerin gerçekleşmesi durumunda aksiyona dönüştürülmesi, risk yönetimini iyileştirmek için düzenli kontrol veya gözetimin sağlanması, mevcut risklerin gelişmelere bağlı olarak değişiklerinin tespit edilmesi ve yeni risklerin belirlenmesi kamu ve özel sektör paydaşları tarafından devamlı olarak uygulanmalıdır. Örneğin Alman Federal Bilgi Güvenliği Ofisi'nin (BSI), siber güvenlik analizlerinin bir parçası olarak, endüstriyel kontrol sistemlerinin karşı karşıya olduğu en kritik risklerin listesini güncelliğini sağlamada bu manada risk yönetimi alanında başarılı uygulamalardan biri olarak verilebilir. Hesaplamalar sırasında tutarlı sonuçlar elde edebilmek için, gerçek veritabanlarından faydalanılarak tüm olaylar analiz edilir.[74]

Herhangi bir riskin gerçekleşmesi durumunda ise kriz yönetimi planının hazır bulundurulması gerekir. KÖİ uygulamalarında bir kriz yönetim planı başlıca şu adımları içerir; bir krizin belirlenmesi; krize uygun müdahalelerin planlanması; krizin yönetilmesi ve en kısa sürede çözülmesi. Kriz yönetimi konusunda tek bir kuruma birincil sorumluluk ve yetki verilmelidir. Kriz meydana geldiğinde yapılacak eylemler bu kurum tarafından belirlenmelidir. Ayrıca kurum tüm eylemleri koordine etmelidir. ABD'de CISA tarafından kurulan 'Ortak Siber Savunma İş Birliği' (JCDC) son yıllarda yaşanan siber saldırılar konusunda kriz yönetimi ile ilgili büyük faydalar sağlamıştır. Aralık 2021'deki Log4J krizi de dahil olmak üzere, JCDC'nin federal kurumların ve özel sektör ortaklarının bazı büyük siber güvenlik saldırılarını hafifletmesine yardımcı olmuştur. Buna ek olarak, Rusya'nın Ukrayna'yı işgaline ilişkin Shields Up kampanyasının kontrol altında tutulması siber saldırılar noktasında tahribatı minimuma indirirken, Daxin kötü amaçlı yazılımının deşifre edilmesi konusunda da aktif rol alarak yaşanması muhtemel başka bir krizi de önlemiştir. Alınan tüm bu başarılı sonuçlar sonrasında, JCDC ayrıca ABD'de ileride yapılacak seçimler için ülkenin elektronik seçim altyapısını ulus devlet tehditlerinden korumak için çalışmaktadır.[75]

Diğer ülke örneklerine bakıldığında, AB tarafında Avrupa Siber Güvenlik Örgütü (ECSO) KÖİ modelinde 2016 yılında kurulmuştur. ECSO, ulusal kamu idarelerinin temsilcilerini bir araya getirmekte olup aynı zamanda özel sektörden girişimlerin de katkısına açıktır. ECSO'nun bir diğer önemli amacı ise; araştırma ve geliştirme alanındaki yatırımları da sağladığı fonlar ile desteklemektir. Bu amaçla projeleri pek çok ülkede finanse eden Horizon 2020 altında yer alan siber güvenlik projeleri ECSO tarafından yürütülmektedir.[76]

Yukarıdaki saptamalara Türkiye açısından bakıldığında, ülkemizde de kritik altyapıların siber saldırılara karşı korunması amacıyla bir KÖİ modeli kurgulanırken paydaşlar arası işbirliğini teşvik eden kurumsal

[73] National Emergency Security Agency, Maritime Cyber Security Report, https://www.huoltovarmuuskeskus.fi/files/d60cfd87d66aa5321cfc9e48dc76f8b5789603b3/maritime-cybersecurity-report.pdf, 01.01.2021
74 BSI, ISM Cyber Security, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KRITIS/ISM_Cyber_Security.pdf?__blob=publicationFile&v=1, 01.08.2020
[75] Axios, CISA director plans proactive cybersecurity for at risk companies, https://www.axios.com/2022/08/10/cisa-director-jen-easterly-vision-for-jcdc, 10.08.2022
[76] ECSO, Cyber Security Made in Europe, https://www.cyberwatching.eu/ecso

bir yapı oluşturulmalıdır ve her bir paydaşın rolü net olarak başlangıç aşamasında belirlenmelidir. KÖİ'nin sürdürülebilir olması amacıyla paydaşlar için ortak temas noktası tanımlanmalıdır, işbirliği süreci boyunca geçerli olacak ilkeler yazılı olarak belirlenmelidir. KÖİ çalışmaları temelinde üretilen siber güvenlik ürünlerinin özelleştirilmiş entegrasyonlara ihtiyaç duymadan dış dünya ile birlikte çalışabileceği açık bir ekosistem olmalıdır. Kurulan ortak siber savunma işbirliği grupları, yeni teknolojilerin getirdiği gereksinimlere uygun olarak endüstriyel kontrol sistemleri ve operasyonel teknoloji üreten, destekleyen ve sunan servisler barındıracak şekilde güncel trendlere uygun olmalıdır. Ayrıca ortaya konan servislerinde test edilebileceği imkanlar doğrultusunda KÖİ paydaşlarının katılımıyla yerel tatbikatlar planlanmalıdır. KÖİ paydaşlarının herhangi birine karşı bir siber saldırı olması durumunda; müdahale başta ilgili kamu kurumları, SOME'ler, saldırıya uğrayan altyapı operatörü ve tüm ekosistem paydaşlarını içerecek şekilde işbirliği içerisinde olmalıdır.

Öte yandan Türkiye'nin mevcut siber güvenlik sistematiği temel olarak Ulaştırma ve Altyapı Bakanlığı çerçevesinde Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde kurulmuş olan Siber Güvenlik Kurulu, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve kurumsal/sektörel olarak kurulan Siber Olaylara Müdahale (SOME) kanalları üzerinden yürütülmektedir. Ancak siber güvenlik stratejisinin uygulanması ve geliştirilmesi, günümüzde siber tehditlerin geldiği aşama itibariyle bilgi teknolojileri çerçevesinin ötesinde asıl olarak ulusal güvenliğin bir meselesi haline gelmiştir. Bu doğrultuda ülkenin siber güvenlik yapısının bütününün, multidisipliner alt kurum ve kuruluşlara sahip güvenlik merkezli bir çatı örgütlenme üzerinden faaliyet göstermesi, faaliyetlerin odağına ulusal güvenliğin koyulması noktasında fayda sağlayacaktır. Bu kapsamda örnek olarak ABD İç Güvenlik Bakanlığı (Departement of Homeland Security) benzeri bir teşkilat yapısı sunulabilir. Bu kapsamda USOM muadili olarak öne çıkan National Cybersecurity and Communications Integration Center/NICIC Homeland Security çatısı altında faaliyet göstermektedir.

Türkiye'nin siber güvenlik yapılanması içerisinde, ülkenin kritik altyapısının siber güvenliğinin sağlanması, siber savunma ve espiyonaj kapasitesinin geliştirilmesi hedefi doğrultusunda faaliyet göstermesi öngörülen kurumlardan birisi de AFAD'dır. Bu kapsamda AFAD, Türkiye'nin maruz kalacağı yüksek yoğunluklu bir siber saldırı ve böylesi bir saldırının, kritik altyapılara verebileceği zarar sonucu oluşması muhtemel bir afet senaryosunda kriz yönetim sürecinin koordinasyonuyla yetkilendirilmiştir. AFAD ,2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi ile siber afet kriz yönetim hedeflerini belirlemiş olsa da 2022 yılı itibariyle hedeflere ulaşılma süreç takibi noktasında herhangi bir rapor yayınlamamıştır. Bu doğrultuda AFAD'ın hangi kurumsal yapılanmayla nasıl süreçler sürdüreceği ve bunun ötesinde böylesi bir siber afet durumunu koordine edebilecek nitelikli personelin kurum bünyesinde mevcut olup olmadığı noktaları soru işareti oluşturmaktadır. 2014-2023 Yol Haritasının sonuna gelinmesi göz önünde bulundurulduğunda AFAD'ın yıl bu yıl sonu itibariyle siber afet durumlarındaki hareket planı ve yol haritasında konan hedeflerin kontrolü noktasında genel nitelikli bir rapor yayınlamasında fayda bulunmaktadır.

Siber güvenlik alanına dair temel bir ihtiyaç da insan kaynakları açığı olmaya devam etmektedir. Bu bağlamda geliştirilebilecek eğitim politikaları iki ana başlık altında ele alınabilir. Bunlardan ilki ihtiyaç duyulan nitelikli iş gücünün geliştirilmesi yoluyla siber güvenlik uzmanı arzının sağlanabilmesidir. Diğer taraftan günümüzde siber alanın hayatın her alanına nüfuz ettiği göz önüne önüne alındığında, yaş, kademe, pozisyon, sektör fark etmeksizin internet kullanıcılarının tümünün potansiyel risk ve tehditler hususunda belirli bir farkındalık seviyesine ulaşması ise ikincil önemli başlık olarak karşımıza çıkmaktadır.

Günümüzde yükseköğretimde siber güvenlik formasyonunun henüz arzu edilen noktaya gelemediği globalde genel kabul edilen bir varsayım olarak karşımıza çıkmaktadır. Hem nitelik hem nicelik olarak geride kalan bu tarz programların arzını sağlayamadığı siber güvenlik uzmanlarını yetiştirebilmek için Facebook, Google, Bloomberg gibi şirketlerin kendi içlerinde siber güvenlik eğitim programları oluşturarak yazılımcı/geliştiricileri siber güvenlik alanına kaydırmayı hedefliyor olmaları akademideki

eksiliği daha görünür kılmaktadır. Türkiye'de de CCI benzeri büyük ölçekli şirketler uzman pozisyonları doldurabilmek için benzer yöntemler uygulamaktadır. Akademide mevcut bu eksikliğin giderilmesi için halihazırda Yüksek Öğretim Kurumu (YÖK) ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi öncülüğünde girişimler mevcuttur. Bu kapsamda siber güvenlik alanında ilk olarak ülkemizde 11 Adet yüksek lisans programı ve 1 adet doktora programı açılmış bulunmaktadır. Bu programları 2 senelik ön lisans ve 4 senelik siber güvenlik lisans programlarının takip etmesi beklenmektedir.

Ancak anılan program içerikleri incelendiğinde yalnızca 1 adet vakıf ve 1 adet devlet üniversitesi mezun programının İngilizce olarak eğitim sağladığı göze çarpmaktadır. Bu kapsamda siber güvenlik tehditlerinin sınır tanımaz niteliği ve alanın doğası göz önüne alındığında, bu alanda ihtisas sahibi olacak adayların siber alandaki en yaygın dil olan İngilizceye hâkim olmalarını beklemek doğaldır. Sonuç olarak özellikle lisans, yüksek lisans ve doktora programları müfredatında İngilizceye ayırılan payın arttırılmasında, tercihen formasyon dilinin olabildiğince İngilizce 'ye çevrilmesinde fayda görülmektedir.

Ayrıca açılması öngörülen yeni ön lisans ve lisans programları sayesinde sıfırdan siber güvenlikçi yetiştirmenin ötesinde uygulanabilecek bir diğer politika ise mevcut yazılım/bilgisayar mühendisliği eğitimine sahip öğrencilerin kariyer planlamasında siber güvenliği göz önünde bulundurmaları için bazı teşvikler öngörülebilir. Böylelikle halihazırda bilişim alanında entelektüel donanım sahibi genç ve öğrencilerin daha az maliyetli ve daha efektif şekilde siber güvenlik uzmanı olabilmeleri mümkün hale gelecektir. Bu kapsamda YÖK'ün nitelikli eleman ihtiyacı olan kritik sektörleri cazip hale getirebilmek için öğrencilere sağlamakta olduğu destek bursları kapsamına Siber Güvenlik lisans ve yüksek lisans programlarının da alınmasının alanı cazip hale getirme noktasında faydalı olacağı düşünülmektedir. Ayrıca aynı gaye ile uygulanabilecek bir diğer politika ise Cumhurbaşkanlığı İnsan Kaynakları Ofisi eşgüdümüyle faaliyet gösteren Üniversite Kariyer Merkezleri (KAGEM)'ler bünyesinde Siber Güvenlik Kariyer Fırsatları konusunda bilgilendirmeler ve tanıtımlar yapılması yoluyla öğrencilerin alan hakkında bilgilendirilmesi olabilir.

Siber güvenlik alanı aynı zamanda çok taraflı uluslararası örgütlerin de gündemini meşgul etmektedir. Bu kapsamda Birleşmiş Milletler nezdinde 2004 yılından itibaren 6 adet "Bilgi Güvenliği Konusunda Devlet Uzmanları Grubu" (GGE) düzenlenmiş, en sonuncusu 2019 -2021 yılları arasında gerçekleşmiş ve 2021 yılında bir rapor hazırlanmıştır. Türkiye şu ana dek BM içerisindeki siber güvenlik gruplarına katılım sağlamamıştır. Türkiye'nin siber güvenlik alanında uluslararası normların oluşum sürecine müdahil olmaması, çıkan sonuçlarda etkisi olmaması anlamına gelmektedir. Böylelikle Türkiye uluslararası norm oluşum sürecinde kendi siber güvenliğine katkı sağlayacak tasarıları destekleme ve zararlı bulduklarına karşı çıkma fırsatından mahrum kalmaktadır. Türkiye'nin GGE ve BİT güvenliği konusunda Açık Uçlu Çalışma Grubu (2021-2025) gibi BM çalışma gruplarına katılması ve katkı sağlaması bu bağlamda önem arz etmektedir.

BM'nin yanısıra NATO bünyesinde de siber güvenlik çalışmaları sürmektedir. Bu bağlamda NATO'nun Tallinn merkezli siber araştırma ve düşünce kuruluşu Müşterek Siber Savunma Merkezi (CCD COE) bünyesinde Türkiye üye olarak bulunmakta ve 1 askeri 1 sivil temsilci ile temsil edilmektedir. NATO bünyesinde yürütülen siber güvenlik projelerinin bir diğeri ise Siber Çatışma Hukuku hakkında öncül nitelik taşıma potansiyeline sahip düzenlemeler yapılması olmuştur. Bu kapsamda yayınlanan Tallinn El Kitabı'nın güncellenerek Tallinn El Kitabı 2.0'ın yayınlanması beklenmektedir. Türkiye, BM içerisinde yürütülmesi tavsiye edilen bir politikanın benzerini uygulayarak savaşın bu yeni alanının çatışma hukukunun düzenlenmesinde milli güvenlik prensiplerini göz önünde bulundurarak etki etmeli ve Tallinn sürecine dahil olmak için gerekli çalışmaları gerçekleştirmelidir. İttifakın her alanına yüksek seviyede katkı sağlayan Türkiye, bu rolünü siber güvenlik alanında da sürdürmelidir.

Türkiye'nin kritik altyapısını korumak ve geliştirmek için yaptığımız çalışmaların sonunda özetle 6 önemli aksiyon öne çıkıyor:

1 - Kritik altyapıların siber saldırılara karşı korunmasına yönelik PPP modeli oluşturulurken paydaşlar arasında işbirliğini teşvik eden kurumsal bir yapı oluşturulmalı ve her bir paydaşın rolü başlangıç aşamasında net bir şekilde tanımlanmalıdır.

2 - Ülkenin tüm siber güvenlik yapısının çok disiplinli alt kurum ve kuruluşlardan oluşan güvenlik merkezli bir çatı teşkilat aracılığıyla işletilmesi, faaliyetlerin merkezine ulusal güvenliğin alınması açısından faydalı olacaktır. Bunun bir örneği ABD'de bulunan ve tüm bakanlıkları bir araya getirerek proaktif bir çalışma ortamı sağlayan İç Güvenlik Ofisi olarak kabul edilebilir.

3- Afet yönetimi için kurumsal yapının hangi noktalarda kullanılacağı ve kurumlar bünyesinde nitelikli personel bulunup bulunmadığı araştırılmalıdır. Ayrıca, ulusal afet yönetim planı, kamu kurumları için kritik altyapının korunmasına rehberlik edecek şekilde periyodik olarak güncellenmelidir.

4- Akademide uzmanlaşma fırsatları geliştirilmelidir. nitelikli iş gücü her geçen gün daha fazla önem kazanıyor. Bu konuda YÖK, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve bakanlıklar arasında işbirliği olanakları artırılmalıdır. YÖK ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi arasında siber güvenlik ve ağ yönetimi meslek yüksekokullarının kurulmasına ilişkin anlaşma buna güzel bir örnek olabilir. Bu tür işbirliklerinin gelişmesi için uygun ortam sağlanmalıdır.

5- Birleşmiş Milletler ve benzeri örgütlerde siber güvenlik gruplarına katılım sağlanmalıdır. Uluslararası siber güvenlik normlarının oluşmasına katkıda bulunmak Türkiye için bu konuda kritik önem arz ediyor. Türkiye bu alanda söz sahibi olmak istiyorsa uluslararası platformlarda üretken, işbirlikçi ve paylaşımcı olmaya özen göstermeli ve ivmesini artırmalıdır.

6- Türkiye, milli güvenlik ilkelerini dikkate alarak küresel hukuki süreçlerde yer almalıdır. Türkiye'de başta KVKK olmak üzere katı veri ve bilgi güvenliği yasaları vardır. Özellikle uluslararası proje ve işbirliklerinin geliştirilmesinde kanunlar arasındaki farklılıklar engel oluşturmaktadır. Bu alanda yeni bir yapılanma var ve uluslararası alanda NIS Direktifi 2, Tallinn Manual 2.0 gibi önemli yol gösterici belgelerden yararlanılarak dinamik bir düzenleme süreci oluşturulmalıdır. Bu sayede yasalar, siber uzayda geliştirilecek uluslararası hizmetlerde engel değil yol gösterici ve destekleyici bir rol oynayabilir.

KÜNYE

Yazar: Uğur Özker

Uğur Özker, IBM Orta Doğu ve Afrika'da Kıdemli Çözüm Mimarı olarak çalışmalarına devam ediyor. Yapay Zeka, Büyük Veri, Siber Güvenlik ve Danışmanlık alanlarında 12 yılın üzerinde tecrübesi bulunuyor.

2012 - 2014 yılları arasında bir teknoloji geliştirme merkezinde çeşitli Ar-Ge çalışmalarının ardından, 2014-2018 yılları arasında akıllı şehir, elektronik ücret toplama/satış noktası sistemleri ve IoT cihazları konularında birçok global projede yazılım mimarı olarak görev almıştır. Ardından Türkiye'nin en büyük kamu bankasının teknoloji merkezinde Fintek alanında yeni teknolojilerin geliştirilmesi için araştırma ve geliştirme uzmanı olarak birçok başarılı siber güvenlik, yapay zeka & büyük veri projesinden sorumlu oldu.

Bilgisayar Mühendisliği alanında Lisans & Yüksek Lisans derecesi ile mezun olan Özker, İşletme Yüksek Lisans derecesine de sahiptir. Project Management Institute tarafından verilen uluslararası PMP sertifikası sahibidir. Ayrıca Agile/Scrum teknikleri ile başarılı BT proje yönetimi tecrübesine de sahiptir.

Yazar hakkında daha fazla bilgiye LinkedIn profilinden ulaşabilirsiniz.

Bu yayın yalnızca yazarın görüşlerini yansıtmaktadır.

Konrad-Adenauer-Stiftung e.V. & Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM)

Walter Glos
Direktör
Türkiye Ofisi
walter.glos@kas.de

Tacan Ildem
Başkan
EDAM
tildem@edam.org.tr