reflektif
SOSYAL BİLİMLER DERGİSİ
JOURNAL OF SOCIAL SCIENCES

Reflektif Journal of Social Sciences, 2025, Vol. 6(1)

2025, Vol. 6(1), 59-80

DOI: 10.47613/reflektif.2025.202
Article type: Research Article

Received: 14.01.2025
Accepted: 06.02.2025
Published Online: 25.02.2025

Salih Bıçakcı*, Ayhan Gücüyener Evren**

Sihirli Reçete mi, Kara Kutu mu: Siber Krizlere Karşı Esnek-Dayanıklılık Anlatısının İncelenmesi

A Magic Recipe or Black Box: Investigating the Narrative of Resilience for Cyber Crises

Öz

Gelişen dijital teknolojiler ve buna eşlik eden sosyo-ekonomik dönüşüm siber güvenlik krizlerini çoklu krizler döneminin bir parçası haline getirmiştir. Bununla beraber, siber tehdit aktörlerinin ve saldırı yöntemlerinin dinamik doğası, riskleri modellemenin ve saldırıların etkisini tahmin etmenin zorlukları, siber güvenlikte belirsizliği ve güvenliksizliği adeta bir norm haline getirmiştir. Bu çerçevede, siber esnek-dayanıklılık son on yılda siber güvenlik alanında en geçerli paradigmalardan birine dönüşmüş ve krizlerde hayatta kalabilme ve adaptasyon yeteneklerini vurgulayan bir çözüm olarak öne çıkmıştır. Öte yandan, siber esnek-dayanıklılık tek bir çözüm, teknoloji ya da uygulama değildir; esasen sosyo-teknik çözümlerin bir denge içinde uygulanmasını gerektiren çok katmanlı bir yaklaşımdır. Bu çerçevede, araştırmamızda siber esnek-dayanıklılık kavramını siber güvenlik kavramından ayırarak detaylı olarak anlamayı ve bu kavramı özellikle siber güvenlik krizlerinin farklı evreleri için insan-süreç-teknoloji yaklaşımı bağlamında ele almayı hedefliyoruz. İlaveten çoklu krizler çağında siber esnek-dayanıklılığın yaklaşımının derinleştirilebilmesi için nasıl daha erişilebilir, esnek, çevik ve kapsayıcı bir siber güvenlik yaklaşımı geliştirebiliriz sorusunu masaya yatırıyoruz.

Abstract

Emerging digital technologies and the accompanying socio-economic transformation have made cybersecurity crises an integral part of the era of poly-crises. Furthermore, the evolving characteristics of threat actors and attack methodologies in cybersecurity, along with the complexities of risk modeling and the problems of forecasting attack impacts, have rendered uncertainty and insecurity in this domain nearly normative. Within this framework, cyber resilience has become one of the most prominent paradigms in cybersecurity over the past decade, emphasizing survival and adaptation capabilities during crises. However, cyber resilience is not a single solution, technology, or application; instead, it is a multi-layered perspective that requires the balanced implementation of socio-technical solutions. In this context, by highlighting its differences from cybersecurity, this study aims to explore the concept of cyber resilience in detail and examine it specifically within the dimensions of people, process, and technology approaches for the different phases of cybersecurity crises. Additionally, we address how cybersecurity can be made more accessible, flexible, agile, and inclusive to enhance cyber resilience in the era of poly-crises.

Anahtar Kelimeler

Siber güvenlik, siber esnek-dayanıklılık, sosyo-teknik siber güvenlik, siber güvenlik krizleri, kritik altyapılar

Keywords

Cybersecurity, cyber resilience, socio-technical cybersecurity, cybersecurity crises, critical infrastructures

* Kadir Has Üniversitesi, asbicakci@khas.edu.tr, ORCID: 0000-0002-0143-5255.

** Kadir Has Üniversitesi, ayhan.gucuyener@khas.edu.tr, ORCID: 0000-0002-8140-5864.

Giriş

2021'de 7 Mayıs sabahı, Amerika'nın doğu yakasındaki dizel, benzin ve jet yakıtı ihtiyacının %45'ini karşılayan boru hattı operatörü Colonial Pipeline şirketinin kontrol odasında her şey sıradan görünüyordu. Kontrol odasındaki görevliler her gün 2,5 milyon varillik yakıt akışını izliyordu. Fakat öğle saatlerine doğru bilgisayar ekranlarında dosyaların şifrelendiğini, verilere erişimin engellendiğini belirten ve bütün bunların eski haline gelmesi için kripto para talep eden bir fidye notu belirdi. Daha sonra DarkSide adlı bir siber suç grubunun gerçekleştirdiği anlaşılan bu fidye yazılım saldırısı, şirketin tüm operasyonlarını durdurmasına neden oldu ve bu saldırı eşi görülmemiş bir krizi tetikledi (Petrosyan, 2021). Saatler içinde bu olayın etkileri ekonomiyi sarsmaya başladı. Doğu Yakası'ndaki benzin istasyonlarında, halkın yakıt kıtlığı korkusuyla panik alışverişine başlamasıyla yakıt tükendi. Hafta sonunda, akaryakıt fiyatları yıllardır görülmeyen seviyelere yükseldi ve bu da pandemiyle zaten zor durumda olan tüketicilerin mali yükünü daha da artırdı. Etkiler sadece bununla sınırlı kalmadı: Yakıt tedarikine bağımlı işletmeler aksaklıklarla boğuştu, havayolu şirketleri artan jet yakıtı maliyetlerine hazırlanmaya çalıştı ve lojistik ağlar bu duruma uyum sağlamakta zorlandı. Colonial Pipeline'ı hedef alan olay sadece bir siber saldırı değildi; öte yandan kritik altyapıların kırılganlığını ve çoklu krizler çağında karşı karşıya kalınabilecek zorlukları acı bir şekilde hatırlattı. Aynı zamanda bu olay tek bir başarısızlık noktasının ulusal bir krize nasıl dönüşebileceğini, yalnızca enerji sektörünü değil, aynı zamanda kamu güvenini, jeopolitik dengeleri ve ekonomik direnci nasıl etkileyebileceğini gözler önüne sererek esnek-dayanıklılık (*resilience*) uygulamalarının karşılıklı bağımlılığın kaçınılmaz olduğu bir dönemde bir seçenek değil zorunluluk olduğunu da ortaya koymuş oldu.

Colonial Pipeline'ı hedef alan olay son yılların en çok konuşulan fidye yazılımı saldırılarından biri olsa da karşılaşılan tek örnek değildir. Nitekim, toplumlara kritik hizmetleri sunan altyapıların dijitalleşmesiyle siber krizlerin şiddeti de artmaktadır. Karşılıklı bağımlılık, farklı krizlerin etkileşim içine girerek birbirlerinin etkilerini öngörülemez ve doğrusal olmayan şekilde etkilemesine uygun bir ortam hazırlamıştır. Buna ek olarak, küresel sistemde olduğu gibi siber-fiziksel ortamlarda da farklı aktörler, çıkarlar, sistemler ve değerler birbiriyle iç içe gelmiş haldedir. Bütün bunlar görünürlüğü azaltarak ve kakofoniyi arttırarak krizlerin yönetilmesini güçleştirmektedir. Örneğin müşterilerinin kimlik bilgileri çalınan bir kurum için öncelik kurumun itibarının korunmasıyken, siber güvenliğe ilişkin mevzuat bu olayın hızlı ve şeffaf şekilde kamuya duyurulmasını gerektirebilmektedir. Siber ve kinetik sistemlerin birlikte çalışmasından doğan karmaşıklık krizlerin niteliğinin ve potansiyel etkilerinin anlaşılmasını da zorlaştırmaktadır. Bununla beraber, siber güvenlik yapılarının kendi doğalarındaki karmaşıklık siber esnek-dayanıklılığı olumsuz yönde etkileyebilmektedir. Örneğin, bir kurumun siber güvenlik mimarisinde farklı tedarikçilerden edinilen teknolojilerin varlığı söz konusuysa siber olaylara müdahale edebilmek için koordinasyon ve tedarikçi yönetimi elzem hale gelmektedir.

Dahası bu çok paydaşlı yapıda sistemleri tekrar işler hale getirmek için alınması gereken tedbirlerin ne olduğunu tahmin etmek bile güçleşmektedir.

Hızlı dijital dönüşüm ve Yapay Zeka (YZ) gibi teknolojilerin saldırganlara yeni olanaklar sunması da bu gelişmelerle beraber değerlendirildiğinde belirsizlik siber güvenlikte birincil sorun haline gelmiştir. Kurumlar her ne kadar yatırımlarla siber güvenliğe ilişkin önlemler almaya çalışsalar da siber tehditlerin dinamik doğası ve saldırıların etkilerini öngörmenin güçlüğü, risk yönetimi yöntemlerini siber güvenlik açısından yeterince etkili olmayan bir pratik haline getirebilmektedir. Bu eksikliğe binaen, Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü'nün de tanımladığı gibi, siber tehditlere karşı "dayanma, hızlı toparlanma, zarar azaltma, uyum sağlama, adaptasyon" gibi yeteneklerin kazanımıyla örtüşen "siber esnek-dayanıklılık" (*cyber resilience*) kavramı sihirli bir reçete olarak sunulmaktadır (National Institute of Standards and Technology, 2024).

Siber esnek-dayanıklılık bir sonuç değil süreçtir ve her krizin oluşumuna sebep olan nedenler, organizasyonel yapının kriz anındaki işleyişi gibi birçok faktöre bağlıdır. Temel anlamıyla siber esnek-dayanıklılık her şeyden önce siber güvenliği sağlayan unsurların işlevselliğin korunmasına odaklanır. Bununla beraber, siber esnek-dayanıklık yekpare bir reçete olmaktan ziyade bir alet kutusu olarak değerlendirilmelidir. Bu alet kutusunda, kriz iletişiminden, insan kaynağı yönetimine; liderlikten adaptasyona kadar teknolojik, sosyal ve kurumsal kültüre ilişkin birçok farklı bileşen bulunmaktadır. Bir başka deyişle, siber esnek-dayanıklığın sağlanması ancak bu farklı katmanların doğru oranlarda bir araya getirilip çalıştırılabilmesiyle mümkündür. Bu varsayım aynı zamanda siber esnek-dayanıklılığı sağlamanın evrensel bir yöntemi olmadığı ön kabulünü de beraberinde getirmektedir.

Bu çalışmadaki kavramsal yaklaşımımıza açıklık getirmek gerekirse, İngilizce'de *resilience* kelimesinin Türkçe'ye hızlıca dayanıklılık, direnç gibi kelimelerle çevrilmesinin bilişsel bir yanılgıya yol açtığını düşünüyoruz. Resilience kelimesi fizikte elastikiyet, sıkıştırmadan sonra orijinal şekline dönme gücü olarak tanımlanır. İlk haline dönebilme niteliği esneklikle yakından ilişkilidir. Öte yandan Türkçedeki dayanıklılık ve direnç kelimeleri bir güce karşı "dayanıklı olma durumu" olma şeklinde tanımlanmıştır. Belirli bir gücü taşıyabilmekle gücün etkisini taşıyıp tekrar ilk haline dönebilmeyi ifade eden bir esneklik yoktur. O yüzden resilience kelimesini esnek-dayanıklılık olarak tanımlamanın daha yerinde olacağını düşünüyoruz. Bu bilgiler ışığında bu makalede, siber esnek-dayanıklılık kavramını, siber güvenlikten farklarını ortaya koyarak incelemeyi, siber esnek-dayanıklılık kavramını oluşturan katmanların başlıcalarını değerlendirmeyi ve nihai olarak siber esnek-dayanıklılığa ilişkin kavramsal tartışmaları sosyo-teknik bir düzlemde zenginleştirmeyi hedefliyoruz. Öncelikle siber esnek-dayanıklılık anlatısını kaçınılmaz hale getiren belirsizlik kavramından bahsetmeyi, ardından, siber esnek-dayanıklılığı oluşturan alet çantasının sosyal ve teknolojik katmanlarının önemli unsurlarını, özellikle toplumsal sonuçlar doğurabilecek ve kritik altyapıları tehdit eden siber güvenlik riskleri çerçevesinde mercek altına almayı amaçlıyoruz. Son olarak, tartışmamızı kapatırken,

çoklu krizler çağında nasıl daha zengin bir siber esnek-dayanıklılık anlayışının ortaya koyulabileceğini anlamayı hedefliyoruz.

Siber Güvenlikte Belirsizlik ve Esnek-Dayanıklılık Kavramı

Üretim ve hizmet sektöründeki maliyetlerin azaltılması ve verimliliğin arttırılması için dijital teknolojilere yapılan yatırımlar artmaktadır. 2030 yılında, sensörler ve yazılımlar aracılığı ile birbirleriyle konuşabilen ve kendi içlerinde bağlantılı cihazlar ve sistemler anlamına gelen Nesnelerin İnternet'inin sayısının 32.1 milyara (Statista, 2024), küresel ölçekte internet kullanıcılarının sayısının ise 7.5 milyara ulaşacağı tahmin edilmektedir (Morgan, 2018). Öte yandan, dijital teknolojiler her ne kadar toplumlar ya da ekonomiler için önemli faydalar sunsa da beraberinde yeni zafiyetleri de getirmektedir.

Ransbotham, Fichman, Gopal ve Gupta'ya göre bu zafiyetler "artan görünürlük", "gelişmiş gizleme", "artan karşılıklı bağımlılık" ve "düşen maliyetler" olmak üzere dört ana unsurla değerlendirilebilir (Ransbotham vd., 2016). Artan görünürlük teknolojilerin ve varlıkların saldırı yüzeyini artırarak saldırganlara hedef olma ihtimallerini arttırırken, internetin anonimliği destekleyen mimarisi de kötü niyetli aktörlerin kendilerini kolayca gizlemelerine imkân tanımaktadır. Artan karşılıklı bağımlılık bir yandan sosyal etkileşimi hızlandırmış, öte yandan, cihazlar, insanlar ve organizasyonların birbirlerinin zafiyetlerinden etkilenme ihtimalini kuvvetlendirmiştir. Düşen maliyetler ise yeniliğe erişimi kolaylaştırarak demokratikleştirme sağlarken, aktörlerin Üretken Yapay Zeka (*GenAI*) ya da Kuantum Bilgisayarlar gibi yeni teknolojileri zararlı faaliyetler için kullanımını da kolaylaştırmıştır (Ransbotham vd., 2016, ss. 2-4). Bu gelişmelerin sonucunda dijitalleşme dalgası siber güvenlik riskleriyle beraber anılmaya başlamış, siber güvenliğin sağlanması için yatırımlar hızlanmıştır. Örneğin, Dünya Ekonomik Forumu'nun 2024 Siber Güvenlik Raporu'na göre, siber güvenlik ekonomisi dünya ekonomisinden 2022 yılında iki kat, 2023 yılında ise dört kat daha hızlı büyümüştür (World Economic Forum, 2024).

Siber saldırıların etkisi ve maliyeti artış göstermektedir. Örneğin, Ukrayna'da 2015 yılında gerçekleşen bir siber saldırının yol açtığı elektrik kesintisinde 225.000'den fazla insan etkilenmiştir (BBC, 2016). Siber suçların yarattığı yıllık maliyetin ise 2025 yılında 10,5 trilyon dolara ulaşacağı tahmin edilmektedir (Morgan, 2018). Sayısal sistemlerin fiziksel sistemlerle bütünleşik hale gelmesi karmaşıklığı arttırmış ve saldırı yüzeyini genişletmiştir. Bu durum siber saldırıların ya da zafiyetlerin nerede ve ne zaman oluşacağını tahmin etmeyi zorlaştırmaktadır. Öte yandan siber sistemler kinetik dünyadaki etkileri nispetinde etkilidir. Dolayısıyla siber esnek-dayanıklılık kavramı siberin altını çizse bile esnek-dayanıklığın gerçekleştiği alan kinetik alanın ve siber uzayın keşişim noktasını kapsamaktadır.

Bununla beraber, siber uzayın kendine has özellikleri, siber tehditlerin fiziksel/kinetik tehditlerden ayrışmasına da sebep olmuştur. Örneğin, siber tehditler gözle görülebilen ya da

sayısal olarak ölçülebilen unsurlar taşımamaktadır. Bu durum, karar vericilerin tehdit değerlendirmesi yapması için gerekli olan somut bilgileri toplanmasını güçleştirmektedir. İnternet, tehdit aktörlerinin kimliklerine ulaşmanın zorluğunun yanı sıra aktörlerin kapasite ve niyetlerine ilişkin bir değerlendirme yapmayı da zorlaştırmaktadır. Nitekim, kötü amaçlı geliştirilmiş bir kodun, espiyonaj için mi yoksa bir kritik altyapıyı kullanılamaz hale getirmek için mi kullanılacağını ayırt etmek güçtür (Brantly, 2021). Öte yandan, siber uzayın kinetik dünyadaki birçok sistem ile iç içe geçmiş olması bir siber saldırının bir düğümdeki etkisinin hızlıca diğer altyapılara sıçrayabilme potansiyeli olarak da adlandırılan "çağlayan etkisi" (*cascading effect*) riskini de beraberinde getirmiştir (Palleti vd., 2021). Çağlayan etkisi özellikle siber saldırıların toplumsal sonuçlarını anlamak bağlamında değerlidir. Siber uzayın farklı düzlemlerdeki aktörleri birbirine bağlayan doğası bir noktadaki kırılmanın zincirleme etkisini ortaya koymaktadır. Örneğin, WannaCry saldırısı sağlık sektöründe yarattığı etkilerle bireylerin hayatını ve toplumun düzenini doğrudan etkilemiştir. Colonial Pipeline örneğinde olduğu gibi Fidye Yazılım saldırıları toplumu genel davranış kalıplarının dışına çıkararak hareket etmesine de sebep olabilir. Siber saldırılar nedeniyle işlevsiz kalan sistemlerin toplumun işleyişini de derinden etkilediği gözlemlenmektedir. Dolayısıyla siber güvenlik sadece ekonomik ya da ulusal güvenlik bağlamında değil, dolaylı da olsa toplumsal etkileri çerçevesinde ele alınmalıdır.

Bütün bu hususlar beraber düşünüldüğünde, siber saldırıların nasıl, nerede, ne zaman gerçekleşeceği ve dahası hedef alınan sistemlerin hangi zafiyetleri barındırdığına ilişkin bilinmezler siber güvenlikte belirsizlik anlatısının önünü açmıştır (Scala vd., 2019). Belirsizlik olgusuna, "tahmin edilemezlik" ve "hızlı değişim" dinamiklerinin de eklenmesi siber güvenlik için kullanılan risk değerlendirme modellerinin yetersiz kalmasına neden olmuştur. Siber güvenlik dünyası bu açığı yeni bir kavram olan esnek-dayanıklılık ile doldurmuştur.

Kökenlerini ekoloji disiplininden alan esnek-dayanıklılık kavramı sadece siber güvenliği kapsamamaktadır. Nitekim, "hızla değişen, karmaşık ve beklenmeyen gelişmelerin olduğu" bir evrende adeta bir "süper kahraman" statüsüne kavuşmuş (Dunn Cavelty vd., 2015, s. 4), iklim değişiminden terörizme tüm güvenlik ve yönetişim sorunlarına neredeyse evrensel bir çözüm olarak sunulmaya başlamıştır. (Aradau, 2014). Kavram, siber güvenlik alanında da son yıllarda ayrıcalıklı bir yere kavuşmuştur. Bir başka deyişle, siber güvenlik alanında tehditlere odaklanmış "savunma" ve risklere odaklanmış "önleme" politikaları yetersiz kalırken, belirsizliklere odaklanmış esnek-dayanıklılık, "adaptasyon" ve "reform" vaadiyle siber güvenlik tartışmalarında yer bulmaya başlamıştır (Juntunen & Virta, 2019, s. 74). Siber güvenlikte esnek-dayanıklılık özellikle 2000'li yılların başından itibaren daha fazla ilgi görmeye başlamış, 2010 yılından sonra ise bu ilgi somut politikalara evrilmeye başlamıştır.

Siber esnek-dayanıklılık kavramının evrensel olarak kabul edilmiş tek bir tanımı yoktur. Tzavara ve Vassiliadis çalışmalarında 2012-2023 yılları arasında 19 farklı siber esnek-dayanıklılık tanımı yapıldığından bahsetmiştir (Tzavara & Vassiliadis, 2024). Bu farklı tanımlar, siber esnek-dayanıklılığın farklı ve muğlak yorumlanmasına sebep olurken, en kapsamlı ta-

nımlardan birisi MITRE tarafından "siber sistemler ya da bunlara bağlı misyonların, gelişmiş siber tehditleri tahmin edebilmesi, bu tehditlerle karşı karşıya geldiği zaman işlevselliklerini koruyabilmesi, onlardan kurtulabilmesi ve bu tehditlere daha iyi cevap verebilmek için adapte olup evrilebilmesi" olarak yapılmıştır (Bodeau vd., 2015, s. 7). Bu tanımdan da anlaşılacağı gibi, siber esnek-dayanıklılık sistemsel bir yaklaşım sunmaktadır. Her siber sistemin farklı şekilde tasarlanması, esnek-dayanıklılık planlarının da farklı olarak kurgulanması ihtiyacını doğurmaktadır.

Eklemek gerekir ki siber esnek-dayanıklılık esasında siber güvenliği karşısına değil içine alan bir kavram olarak karşımıza çıkmaktadır. Örneğin siber güvenlik, internete bağlı sistemlerin ve Bilgi Teknolojilerinin siber tehditlere karşı korunmasına yoğunlaşırken, siber dayanıklılık bu unsurları korumanın yanında iş sürekliliği, yani bir tehdit meydana gelse de işlevselliğin korunmasına odaklanmaktadır. İki kavram arasındaki en önemli bakış açısı farklılığı, siber esnek-dayanıklılığın mutlak güvenliğin sağlanmasının mümkün olmadığı varsayımına odaklanması ve bir tehdit gerçekleştikten sonra hızlıca işlevselliğin geri kazanımını öncelemesidir. Siber esnek-dayanıklılıkta siber tehditlere karşı korunmada başarısız olunsa dahi bunun kontrollü olması (*safe-to-fail*) yani olumsuz etkilerin sınırlanabilmesi beklenmektedir (Björck vd., 2015)

Siber esnek-dayanıklılık ve siber güvenlik ayrı hedefleri olan iki kavram değildir. Siber esnek-dayanıklılık siber güvenliğin yerine getirdiği işlevlerin yeniden işler hale gelmesi şeklinde anlaşılmalıdır. Bir sistemin siber işleyişinin bozulmasına sebep olan her unsurun siber güvenliği de tehdit ettiği düşünüldüğünde, siber esnek-dayanıklılık ve siber güvenliğin birbirinden ayrıştığı durum neredeyse yoktur. Özetle, siber esnek-dayanıklılık, "siber [güvenlik] alan(ın)da meydana gelen olumsuz olaylara rağmen siber güvenliğin sürekliliği sağlamaya yardımcı olan bir araç" olarak görülebilir (Llansó vd., 2021, s. 328). Bu çerçevede siber esnek-dayanıklılıkta temel amaç saldırının etkisinin kısıtlanması yani zararın azaltılmasıdır. Bir başka deyişle, siber uzayda sistemlerin karşılıklı bağımlılık içinde bulunduğu varsayımı ile siber esnek-dayanıklılıkta saldırıların bir zincirleme reaksiyonu başlatmasının önüne geçilmesi hedeflemektedir. Esnek-dayanıklılıkta kısa süreli çözümlerden ziyade uzun dönemde öğrenme ve adaptasyon öne çıkarılır. Siber esnek-dayanıklılık birçok parçayı ve paydaşı ilgilendirdiği için sistem uyumu ve eşgüdümünü gerektirmektedir. Bu sebeple siber esnek-dayanıklık zaman içinde, deneme-yanılma döngüsüyle ve sistemsel uyumluluk içinde tasarlanır.

Siber güvenlik ve siber esnek-dayanıklılık arasındaki farklı bakış açıları kaçınılmaz olarak bu iki kavramın hayata geçirilmesindeki uygulamaların da farklılaşmasını beraberinde getirmektedir. Örneğin, siber güvenliğin sağlanması tehdit aktörlerinin dışarıda tutulmasına yönelik uygulamalar gerektirirken, siber esnek-dayanıklılıkta tehdit aktörünü dışarıda tutma fikri yeterli değildir ve aktörünün içeriye girmeyi başardığı durumun gerçekleşme olasılığı üzerinden planlamalar yapılır (Pearlson, 2024). Siber esnek-dayanıklılık kavramının işleyişinde siber güvenlik sistemlerinin yeniden çalışabilir hale gelmesi önem arz etmektedir. Örneğin fidye yazılım saldırısına uğramış bir petrol boru hattının siber güvenlik sistemlerini tekrar çalışır

hale getirmeden iş devamlılığını sağlamasını beklemek gerçekçi olmayacaktır.

Yine de siber esnek-dayanıklılık hala kapalı bir kutudur. Nitekim, kaçınılmaz belirsizliklere karşı esnek-dayanıklılığın sağlanmasının elzem olduğu öne sürülse de bu kavramın içi tam anlamıyla doldurulamamış ve işleyiş unsurları yeterince açıklanmamıştır. Bu çerçevede, bir sonraki bölümde siber esnek-dayanıklılık kavramını zamansal boyutlarıyla ve siber güvenliğin tamamlayıcı unsurlarına odaklanarak ele alacağız. Bir başka deyişle, siber krizlerden önce, kriz esnasında ve sonrasında siber esnek-dayanıklılığın insan, süreç ve teknoloji boyutlarına değineceğiz.

Siber Esnek-Dayanıklılığın Sosyo-Teknik Katmanları

Sistemsel farklılıklar tek bir siber esnek-dayanıklılık uygulanma biçiminin oluşmasının önüne geçmiştir. MITRE'nin 2015 yılında yayınladığı "Siber Esnek-Dayanıklılık Mühendisliği Çerçevesi", siber esnek-dayanıklılığın "öngörü" (*anticipate*), "direnme" (*withstand*), "geri kazanım" (*recovery*), "gelişme" (*evolve*) olmak üzere dört temel hedefi olduğundan bahseder. Bu dört amaç kurumların siber tehditleri öngörerek hazırlıklı olabilmesine, siber tehditlere rağmen işlevselliklerini sürdürebilmelerine, zorlu bir durum olsa da iş sürekliliklerini koruyabilmelerine ve kendilerini teknik, operasyonel değişikliklerine ya da gelişen tehdit ortamına adapte edebilmelerine ilişkindir (Bodeau vd., 2015).[1]

MITRE'nin geliştirdiği çerçeve siber esnek-dayanıklılığın hem sistem mühendisliği boyutuna hem de uygulanması gereken teknik pratiklere odaklanmaktadır. Sunulan çerçeve farklı ölçekteki organizasyonlar için de kapsayıcı bir yaklaşım inşa etmektedir. Oysa, Christine ve Thinyane'nin ifade ettiği gibi, siber saldırganlar genellikle siber güvenliğin sosyal-teknik bileşenleri arasındaki boşlukları hedef almaktadırlar. Bu çerçevede siber esnek-dayanıklık uygulamalarının da teknolojik çözümleri merkeze koyan bir anlayıştan ziyade sosyal-teknik unsurları beraber düşünen bir yaklaşıma sahip olması beklenmelidir (Christine & Thinyane, 2022),. Kimilerinin siber güvenliğin zayıf halkası olarak tanımladığı insan unsuru siber tehdit aktörleri tarafından sıkça istismar edilmektedir. Sosyal mühendislik tekniklerinden biri olan oltalama saldırıları son kullanıcıların kurumlara, kişilere ya da sistemlere olan güven duygusunu istismar eden güzel örneklerden birisidir.

Siber güvenlik krizleri, siber güvenlik olaylarından farklıdır ve sistemlerin, ekonominin ya da insanların güvenlik ya da emniyetine zarar verebilecek geniş çaplı siber güvenlik olayları gibi düşünülebilir (ENISA, 2024). Siber güvenlik krizlerinin çözülmesi için normal ve günlük prosedürlerin uygulanması yetersiz kalabilir (ANSSI, 2022). Bununla beraber, Avrupa Siber Güvenlik Ajansı'nın (ENISA) da belirttiği gibi, bir siber güvenlik olayını "kriz" olarak adlandırmak daha çok yorumlamayla ilintilidir. Bir başka deyişle, siber olayın siber krize dönme eşiği her kurum için öznel olup daha çok aktörlerin risk iştahı ve tolerans kapasitesine bağlıdır (ENISA, 2024). Ayrıca, siber güvenlik olayı ve krizi arasında keskin bir kavramsal ayrım

yapmak, siber güvenlik olaylarının kolayca krizlere dönüşebilme potansiyelinden dolayı yanılsamalara da sebep olabilmektedir. Yine de özellikle karar vericiler açısından, siber güvenlik krizleri bazı tipik özellikler taşır. Siber güvenlik olayının birden fazla ülkeyi, sistemi ya da altyapıyı etkilemesi, işlevselliğe zarar vermesi, karar verme süreçleri üzerinde zaman baskısı oluşturması, karar verici için birden çok aktörle etkileşim kurma zorunluluğu yaratması ve karar verme ortamındaki yetersiz ya da hızlı bilgi akışı bunlardan bazılarıdır (Bıçakcı & Gücüyener Evren, 2023).

Krizler statik olmayan, ani gelişen ve beklenmeyen gelişmelere meydan veren dinamik olaylardır, dolayısıyla krizleri zamansallık boyutuyla ele almak yönetilebilmeleri açısından önemlidir (Gryszkiewicz & Chen, 2012). Buna bağlı olarak, siber güvenlik krizlerine karşı esnek-dayanıklılık uygulamaları geliştirmek, yalnızca krizin görünür olduğu ana değil, diğer fazlarına da odaklanmayı gerektirir. Bunlar genellikle krize hazırlık, krize cevap verme ve kriz sonrası geri kazanım fazlarını içermektedir. Bu fazlardan her biri siber esnek-dayanıklılık sürecinin bir parçası olarak, insan, süreç ve teknoloji boyutlarına ayrı ayrı odaklanan bir düşünme pratiğini gerektirir. İnsan, süreç ve teknolojiye dair üç boyutu kısaca açmak gerekirse, insan katmanı bir organizasyonun çalışanlarının tümüyle ilgiliyken, süreç boyutu rutin eylemleri şekillendiren stratejiler ile ilgilidir. Teknolojik boyut ise insan ve süreç unsurunun destekleyici kolonudur, bir başka deyişle, bir kurumun işleyişini destekleyen donanım ve yazılım altyapısını kapsayan ekipmanlardır. Bu hususta çalışmanın giriş bölümünde de vurgulandığı gibi, siber esnek-dayanıklılık kavramını tek parçalı mucizevi bir reçete gibi görmektense, bu kavramın temsil ettiği alet kutusunu açmak ve siber krizlerin her bir fazındaki farklı ihtiyaçlardan bahsetmek anlamlı olacaktır. Elbette bu metin çerçevesinde, siber esnek-dayanıklılık öğelerini bütünüyle inceleme fırsatını bulamayacağımız açıktır. Bu çerçevede, özellikle siber krizleri çoklu krizlerle beraber düşündüren, örneğin kritik altyapıları hedef alan ve toplumsal süreçleri etkileyebilen siber saldırılara yönelik esnek-dayanıklılık unsurlarına odaklanılacaktır.

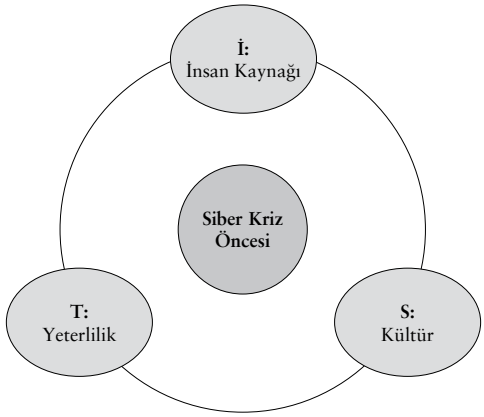
İnsan Kaynağı, Kültür ve Yeterli Sistemler: Siber Krizler Öncesi Esnek-Dayanıklılık

Kriz öncesi dönem siber esnek-dayanıklılık çerçevesinde önleyici tedbirlerin hayata geçirildiği, tehditlerin öngörülerek zarar azaltıcı önlemlerin alınabileceği dönemdir. Bir başka deyişle, bu dönemde aktörlerin siber krizleri göğüsleyebilecek kapasiteyi inşa etmeleri beklenir. Kapasitenin kriz ortaya çıkmadan önce inşası önemlidir, çünkü kriz anında kapasiteyi sıfırdan oluşturmaya çalışmak krizi yönetmek için verilecek yanıtları geciktirebilir ya da kaosa yol açabilir.

Krizler öncesi kapasite inşası yalnızca işlevselliği geri kazanacak teknik altyapının inşası olarak düşünülmemeli, insan kaynağının hazırlanması da esnek-dayanıklılık kapasitesinin unsurları içinde değerlendirilmelidir. Kriz öncesi dönemde insan odaklı hazırlıklar, en az siber güvenlik mimarisinin inşası kadar önemli ve icrası zor bir eylemdir. Altını çizmek gerekir ki siber esnek-dayanıklılık sadece siber güvenlik alanında çalışanlarla icra edilebilecek bir sü-

Şekil 1

Siber Kriz Öncesinde Esnek-Dayanıklılığa İnsan-Süreç-Teknoloji Temelli Yaklaşım



reç değildir. Bu süreçte üst yönetim, insan kaynakları ve halkla ilişkiler bölümlerinin birlikte çalışabilme kabiliyetleri de öne çıkmaktadır. Farklı bölümlerde çalışan insan kaynaklarının temelde aldıkları eğitimler ve problemlere yaklaşımları bilişsel olarak farklılık göstermektedir. İlaveten her insanın krizler sırasındaki davranış biçimleri, stres ile baş edebilme becerileri değişebilmektedir. Çoğu kuruluş bu insan gücünün esnek-dayanıklılık niteliklerini ve birlikte çalışabilme kapasitelerini ölçmez. Bir başka deyişle kriz öncesi kapasite inşasında yalnızca teknik işleyişin devam etmesine odaklanma yanılgısı da krizlerin yönetilmesini güçleştirmektedir. Krizlerin teknik boyutunun ortak ve şeffaf iletişimini zorladığı da düşünüldüğünde siber krizlerin insan boyutunun ne denli önemli olduğu daha net anlaşılacaktır.

Kapasite inşasının diğer boyutu da yetkin siber güvenlik insan kaynağı oluşturulmasıdır. Ancak bu konuda aşılması gereken zorluklar söz konusudur. Dünya genelinde siber güvenlik alanında bir yetenek açığı krizinden bahsetmek mümkündür. ISC2'in son yayınladığı Siber Güvenlik İşgücü Raporu'nda 2024 yılı için 4,763,963 milyon uzman açığından bahsedilmiştir. Öte yandan bu açığın yalnızca uzman sayısının yetersizliğinden kaynaklanmadığı ve ekonomik kaygılarla kurumların siber güvenliğe ilişkin departmanlarında küçülmeye gitmesi, eğitimlere yatırım yapmaması ya da gerekli olsa da yeni işe alım gerçekleştirmemesi de siber esnek-dayanıklılığı zayıflatıcı unsurlar olarak kaydedilmiştir (ISC2, 2024).

Siber güvenlikteki yetenek krizinin bir başka boyutunu da siber güvenlik uzmanlarının yaşadığı tükenmişlik sendromu oluşturmaktadır. Örneğin Sophos'un Asya-Pasifik bölgesindeki siber güvenlik uzmanları özelinde yaptığı bir araştırmada araştırmaya katılan şirketlerin %85'i siber güvenlik çalışanlarında tükenmişlik sendromu gözlemlediklerini kaydetmişlerdir (Sophos, 2024). ISACA'nın 2024'te yaptığı bir araştırmada ise siber güvenlik uzmanlarının %46'sının yüksek stresle baş ettiği tespit edilmiştir (ISACA, 2024). Bu durumun siber güvenlik

gibi yüksek dikkat ve sürekli izleme gerektiren bir uzmanlık alanında yaratabileceği olumsuz etkiler de siber esnek-dayanıklılığın sağlanması çerçevesinde ele alınmalıdır. Siber esnek-dayanıklılığın insan boyutunda siber krize müdahale edebilecek doğru kişilerin bir araya getirilmesi elzemdir. Kriz öncesi dönemde krize kimin müdahale edeceğini belirlemek önemlidir. Eğer bir ekip kurulacaksa bu ekipte kurumun en üst düzey yetkilileri, kriz yöneticisi ve organizasyonun teknoloji altyapısını bilen uzmanların olması gerekmektedir (Bonime-Blanc & Saban, 2021).

Kriz öncesi dönemde insan boyutunun diğer yönünü çalışanların siber güvenlik tehditlerine karşı farkındalığı oluşturmaktadır. Araştırmalara göre, siber güvenlik saldırılarının %80'inden fazlası çalışan hatalarıyla ilintilidir (ESET, 2024). Örneğin 2022'de CISCO'yu hedef alan siber saldırı, bir çalışanın kişisel e-posta bilgilerinin ele geçirilmesi ile başlamıştır (TechTarget, 2022). Giriş bölümünde bahsi geçen, 2021'de Colonial Boru Hattı'nı hedef alan ve enerji güvenliği çerçevesinde değerlendirilen siber saldırı ise bir çalışanın artık kullanılmayan bir hesabına izinsiz erişim üzerinden gerçekleşmiştir (Beerman vd., 2023). Birçok kurum çalışanları için siber güvenlik tehditlerine karşı farkındalık eğitimlerini zorunlu kılmaya başlamıştır. Öte yandan, bu inisiyatiflerin siber esnek-dayanıklılığa anlamlı bir katkıda bulunabilmesi için düzenli olan icra edilmeleri, etkinliklerinin nesnel olarak ölçülmesi ve çalışanların kurum içindeki rollerine ve risk profillerine göre (Aldawood & Skinner, 2018; Hadley, 2023) kurgulanmaları önemlidir. Bir başka deyişle üretim tarafında çalışan bir mühendis ile muhasebe tarafında çalışan bir uzmanın karşılaşacağı siber tehdit senaryoları birbirinden farklı olabilir, bu çerçevede siber güvenlik farkındalık eğitimleri farklı rol ve durumlara göre kurgulanmalıdır.

Siber esnek-dayanıklılığın insan kaynağına dönük boyutlarından birisi de birtakım servislerin dışarıdaki yüklenicilere verilmesidir. Dış yükleniciler bir yandan iç işleyişin bir parçasıdır. Öte yandan ise kurumsal işleyiş kültürünün dışında yer alırlar. Bu ikircikli durum, kriz sırasında insanların ortak çalışma kapasitelerini farklı sebeplerden dolayı hızla düşmektedir. Genelde siber esnek-dayanıklılık için yapılan düzenlemelerde dış yükleniciler dışarıda tutulur ve tatbikatlarda yeterince yer almazlar. Oysa, günümüz iş dünyası şartları ve farklı nesillerin beraber çalıştığı düşünüldüğünde insan kaynaklarındaki rotasyon yani hızlı işe giriş ve çıkış süreçlerinin hesaba katılması da siber esnek-dayanıklılık için büyük önem taşır. Nitekim, yoğun personel dönüşümü gruba sonradan katılan bireylerin kurumun siber esnek-dayanıklılık prensiplerini öğrenmekte geride kalmasına sebep olmaktadır. Özetle, kurum kültürünü içselleştirenler gitmekte ve yeni gelenler eşgüdüm konusunda gerekli tatbikat süreçlerine yeterince katılamamaktadır. Bu hızlı sirkülasyon siber esnek-dayanıklılık kapasitesini etkilemektedir. Günümüz ekonomik şartları siber esnek-dayanıklılık yaklaşımlarının hızlı insan gücü değişimi için çözümler geliştirmesini gerektirmektedir.

Kriz öncesi esnek-dayanıklılığın süreç boyutu ise, krizin yönetilmesi esnasındaki yol haritasının krizin öncesinde yapılmış olması ve kurum kültürünün siber esnek-dayanıklılık unsurlarını yalnızca kriz değil rutin zamanda da içselleştirmesi ile açıklanabilir. Siber kriz yönetim planının varlığı bir kurumun kriz sonrasında hayatta kalmasını veya yok olmasını belirleyecek kadar kritik öneme sahip olabilir (Golandsky, 2016). Planlamada, kriz yönetimi

el kitabının oluşturulması en gerekli adımdır. Kaschner'e göre bu el kitabında krizi yönetecek ekibin belirlenmesi, ekipteki kişilerin rollerin tanımlanmış olması, yetki ve sorumluluklarının açıkça belirtilmiş olması önemlidir. Bu el kitabında krizin başlangıcından bitişine kadar olan prosedürler yer almalı ve krize yönelik farklı senaryolar- örneğin bir siber saldırı sonrası üretim sürecinin sekteye uğraması olasılığı- ele alınmalıdır (Kaschner, 2022). Örneğin, Colonial Pipeline saldırısında, kurumun siber güvenlik olaylarına karşı planları olsa da fidye yazılımı senaryosunun bu planlara eklenmemiş olması esnek-dayanıklılık seviyesi üzerinde olumsuz bir etki yaratmıştır (Greiman, 2023) (Riley, 2021).

Buna ek olarak, kriz anında hayati bir önemi olan kriz iletişiminin nasıl yapılacağı, örneğin hangi mesajların verileceği ya da bu mesajları vermek için hangi platformların kullanılacağı, kriz öncesi planlamalar içinde ele alınmalıdır. Çalışanların siber güvenlik tehditlerine karşı farkındalık sahibi olmalarının yanı sıra, siber güvenliğe ilişkin desteğin kurumun en üst seviyesinden gelmesi ve siber güvenliğin iş yeri emniyeti gibi daimi önem atfedilmesi gereken bir konu olduğuna ilişkin bir bilincin oluşturulması siber esnek-dayanıklılık kültürünün sağlanması adına gereklidir (Kaziukonis, 2024). Kurumlar içinde açık iletişimi destekleyen kanalların oluşturulması siber esnek-dayanıklılık kültürünü sağlamlaştıracaktır.

Son olarak, teknolojinin insan ve sürece ilişkin siber esnek-dayanıklılık unsurlarını desteklemesi ve onlarla uyum halinde olması önemlidir. Bir örnek vermek gerekirse, son dönemlerde siber güvenlik alanında kullanımı artan otomasyon teknolojilerinin özellikle tekrar gerektiren ve zaman alıcı olan log izleme gibi görevlerde kullanımı, insan gücünün daha verimli ve stratejik alanlarda kullanımını sağlayabilir. Bunlara ek olarak, Türkçe'ye "gereğinden fazla bulunma" şeklinde olumsuz bir ifadeyle çevrilen *redundancy* kavramı esasında siber esnek-dayanıklılık anlamında önem taşımaktadır. Zira, bir saldırı ya da kesinti anında önemli fonksiyonları yürüten altyapıların yedekli olması, ulaşılabilir olması ve tek kaynağa bağımlı olmamak siber esnek-dayanıklılığın önemli bir fonksiyonudur. Örneklendirmek gerekirse, verilerin yedeklemelerinin doğru politikalarla yapılması, bulut teknolojilerinin kullanımı, ya da veri merkezleri ve kritik sistemler için güç sistemlerinin yedekli tutulması siber krizler öncesi uygulanabilecek önemli pratiklerdir. Her ne kadar kötü niyetli bir siber saldırıdan kaynaklanmasa da 2024'te CrowdStrike firmasının Falcon yazılımının hatalı güncellenmesi nedeniyle dünya genelinde büyük bir kesintiye sebep olan mavi ekran krizi, tek tedarikçi ya da sisteme bağımlı olmanın doğurabileceği olumsuz sonuçlarını krizin şiddeti, kapsamı ve maliyeti anlamında göz önüne sermiştir (Bıçakcı, 2024).

Liderlik, İletişim ve Karar Vermek: Siber Krizler Esnasında Esnek-Dayanıklılık

Bir siber olayın "siber güvenlik krizi" olarak adlandırılıp operasyonların normale dönmesine kadar geçen süreç, krizin tepe noktasıdır. Siber krizler esnasında esnek-dayanıklılık, zararların asgari seviyeye indirilmesi, itibar ve güvenin muhafaza edilmesi ve rutine en hızlı şekilde dö-

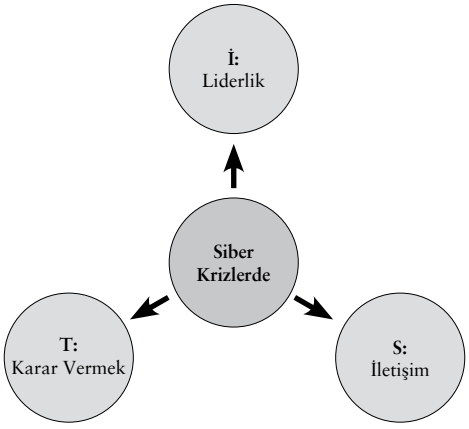
nülebilmesi anlamında önemlidir. **Şekil 2**'de de açıklandığı gibi krize müdahale sürecinin insan boyutunun en önemli unsurlarından biri krizde liderlik, yani krizin yönetimidir. Bir başka deyişle, kriz sürecinden nasıl çıkılacağı krize liderlik edenin vereceği kritik kararlar, sağlayacağı yönergeler ve riskleri taşıma kapasitesine göre şekillenecektir. Siber krize liderlik eden birimin asli fonksiyonu krize müdahaleye ilişkin tüm adımları koordine edebilmektir. Bu çerçevede bu birim kriz iletişimini kontrol altında tutar, bu iletişimde öne çıkarılacak mesajları belirler ve kaynakları koordine eder (Forêt, 2023). Bu görevlerin yanı sıra, krize liderlik edenlerin bazı yeteneklere sahip olması beklenmektedir. Araştırmacılar çalışmalarında kriz esnasında öne çıkan en kritik iki liderlik unsurunu "iletişim" ve "baskı altında karar vermek" olarak ortaya koymuştur (Salviotti & Abbatemarco, 2023).

Norsk Hydro kriz boyunca şeffaflık ve açık iletişim politikası benimsemiş, yöneticiler basın konferansları düzenleyerek müşteriler ve tedarikçiler başta olmak üzere tüm paydaşları saldırının etkisi ve gidişatı konusunda düzenli olarak bilgilendirmişlerdir (Briggs, 2019) (Chatterjee & Hepfer, 2023). Diğer bir örnek de, Equifax Inc.'yi hedef alan ve 145.5 milyon ABD vatandaşının bilgilerinin sızmasına neden olan siber saldırının tespit edilmesinden sonra altı hafta boyunca resmi olarak duyurulmaması tepki toplamış ve kötü bir pratik olarak değerlendirilmiştir (Rapoport & Andriotis, 2017).

Liderlik ile yakından ilişkili olan ancak süreç boyutunu da ilgilendiren en kritik faktörlerden birisi iletişimdir. Kriz iletişimi krizlerde karar verme sürecinin de bir boyutudur; zira krize ilişkin bilgilerin kimlerle ve nasıl paylaşılacağı gibi uzun vadede bir kurumun itibarını etkileyebilecek değerlendirmeleri içerir (Savić & Krivokapić, 2022). Siber güvenlik krizinde iletişim stratejileri, kurumların kriz iletişim stratejisine paralel ilerlese de siber güvenliğe özel düşünülmesi gereken unsurlar taşımaktadır. Örneğin, kriz iletişim planında "yatırımcıların

Şekil 2

Siber Kriz Esnasında Esnek-Dayanıklılığa İnsan-Süreç-Teknoloji Temelli Yaklaşım



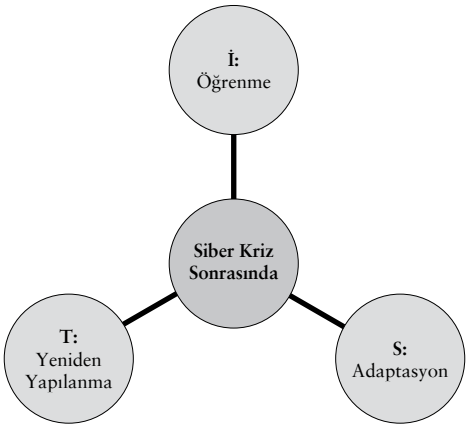
gelişmeler konusunda e-posta ile bilgilendirilmeleri" gibi bir husus yer alabilir ancak bir siber güvenlik krizinde, e-postaların erişilemez duruma gelme olasılığı göz önünde tutulmalıdır (Pearlson & Miller, 2024). Norsk Hydro örneğinde, kurumun web sitesi fidye yazılımı saldırısından dolayı çalışamaz hale gelmiştir; dolayısıyla kriz boyunca sosyal medya kriz mesajlarının paylaşıldığı birincil platform haline gelmiştir (Aoyama vd., 2020). Ek olarak, siber güvenlik krizleri esnasında, "mesajların nasıl paylaşılacağı" hususu önemlidir. Knight ve Nurse çalışmalarında siber güvenlik olaylarından sonra verilecek mesajların "sorumluluğu kabul eden, olayın etkisini önemsiz göstermekten kaçınan, açık ve anlaşılır" olmasının önemli olduğunun altını çizmişlerdir (Knight & Nurse, 2020, s. 19). Son olarak, siber krizler esnasında esnek-dayanıklılığın teknoloji boyutu, krizin tepe dönemindeki en temel iki ihtiyacı, yani hızlı ve doğru karar alabilmeyi desteklemelidir. Bu çerçevede, siber güvenlik krizleri esnasında çoklu kaynaklardan elde edilmiş, doğruluğu ve güvenilirliği saptanabilmiş bilginin önemi ortaya çıkmaktadır. Kurumlar kriz dönemlerinde karar verme süreçlerini hızlandırabilmek için son dönemde karar destek süreçlerine YZ'yı dahil etmektedirler. Öte yandan YZ'daki şeffaflık, açıklanabilirlik ve etik gibi sorunlar YZ'nın krizlerde karar vermeye ilişkin boyutlarını dikkatle incelemeyi gerektirmektedir (Kazemi, 2023).

Adaptasyon ve Öğrenme: Siber Krizlerden Sonra Esnek-Dayanıklılık

Siber krizlerin son fazı operasyonların normale geri döndüğü ve işlevselliğin kriz öncesi seviyeye gelmeye başladığı "iyileşme" sürecidir (Onwubiko, 2020). İyileşme süreci esasen sadece kriz öncesi dönemdeki duruma dönmek değildir. Bunun yanında, krize sebep olan zayıflıkları gözden geçirmek ve siber esnek-dayanıklılığı daha iyi bir seviyeye getirmek için aynı zamanda bir fırsat olarak da görülebilir (Bartock vd., 2016). **Şekil 3**'te gösterildiği gibi, kriz sonrası dönemde siber esnek-dayanıklığın sağlanması krize neden olan hatalardan ders çıkarmaya, öğrenmeye, adaptasyona ve teknolojinin bu dönüşüme yani restorasyona destek vermesiyle mümkündür.

Öncelikle kriz sonrası siber esnek-dayanıklılığın insan boyutuna değinmek gerekirse, krizi deneyimleyen tüm aktörlerin ve paydaşların (örneğin krizden etkilenen tedarikçilerin ve müşterilerin) aynı masada buluşturulması, geri bildirimlerinin toplanması ve bu verilerin adaptasyon sürecinde yeni politikalar ve stratejiler oluşturulurken değerlendirilmesi krizlerden öğrenmenin ilk adımını oluşturmaktadır (Renckens vd., 2024). Bununla beraber, öğrenme sürecinin sürdürülebilir kılınması için oyunlar, etkileşimli tatbikatlar ve simülasyonlar ile siber güvenlik olayları karşısında liderlerin ve yöneticilerin karar verme yeteneklerinin geliştirilmesi ve stres testleri esnek-dayanıklılığın güçlendirilmesi anlamında önemlidir (Hussain vd., 2020; Tonkin vd., 2023). Krizlerden öğrenme sürecinin sağlanabilmesi kurumlarda aynı zamanda kültürel bir dönüşümü de gerektirmektedir; zira çalışanların olumsuz geri bildirimlerinin cezalandırıldığı ve açık olmanın desteklenmediği bir atmosferde siber esnek-dayanıklılıktan da bahsetmek zor olacaktır (Chatterjee & Hepfer, 2023; Patterson vd., 2024). Bütün kriz döne-

Şekil 3
Siber Kriz Sonrasında Esnek-dayanıklılığa İnsan-Süreç-Teknoloji Temelli Yaklaşım



minde yaşanan tüm duraksamaların fatura edileceği bir günah keçisi aranması yaklaşımı da paydaşların kriz sonrası iyileştirme sürecine şeffaf katılımını engelleyecektir.

Krizler değişim için katalizör görevi görebilir. Bir başka deyişle krizlerden öğrenmek, zaman içinde yeni durumlara adaptasyonu da sağlayabilir (Boin & Hart, 2022). Siber esnek-dayanıklılık kavramı da esasen siber güvenliği ilgilendiren bir olaydan sonra ne olduğu ile ilgilenir. Asıl odaklandığı husus, sistemlerin bir siber krize nasıl direndiği değil, bu krizden sonra nasıl davrandığıdır (Kott & Linkov, 2021). Yeni koşullara hızlı adaptasyon yeteneği siber güvenliğin dinamik doğası gereği siber esnek-dayanıklılık fikrinin kalbinde yer almaktadır ve tehditleri daimi olarak izleyip esnek önlemler almayı gerektirmektedir. Öte yandan, siber uzaydaki aktörlerin karşılıklı bağımlılık içinde olması ve saldırıların genellikle bir zincir içindeki en zayıf halkayı hedef alması ekosistemdeki farklı paydaşların beraber çalışmasını yani eş zamanlı bir adaptasyonu da gerektirmektedir (Chatterjee & Hepfer, 2023). Bu çerçevede, örneğin siber tehditlere ilişkin bilgilerin paylaşılabileceği ortak platformlar kurulması siber esnek-dayanıklılığa tehditlere hazırlıklı olması evresinde katkı sağlayacaktır. ABD'de özel sektörden temsilcilerin gönüllük prensibine dayalı katılımı üzerine kurulmuş ve özellikle siber tehdit bilgi paylaşımını hedefleyen Bilgi Paylaşım ve Analiz Merkezleri (ISAC) mekanizması siber güvenlik sektörü için öncül pratikler olarak düşünülebilir (Center for Internet Security, 2024).

Siber krizlerden sonra teknolojiye yönelik çözümler siber esnek-dayanıklılığı desteklemelidir. MITRE'nin siber-esnek dayanıklılık tekniklerinden biri olan koordine savunma, yani farklı siber güvenlik tekniklerinin birbirlerini tamamlayıcı şekilde kullanılması, saldırganın hedefe ulaşmasını mümkün olduğunca geciktirecek ve önleyici tedbirlerin alınmasını kolaylaştırabilecektir (Bodeau vd., 2015). Kurumlar ayrıca siber güvenlik seviyelerini arttırmak için farklı teknolojilere, örneğin daha güçlü doğrulama yöntemlerine, geçiş yapabilirler. Ancak esnek-dayanıklılığın sürdürülebilir kılınması **için**, dijital teknolojilerin inşası sürecindeki yak-

laşımlar da önemlidir. Bir başka deyişle, araçlar ve platformlar geliştirilirken güvenliğin esas olması gereklidir. Bu da güvenliğin ürün geliştirme sonrasında eklenmesinden ziyade teknolojiler ve ürünler geliştirilirken düşünülmesiyle mümkün olacaktır. Güvenlik bakış akışıyla tasarlanmış ürünler artık yasal düzenlemelerin de parçası haline gelmeye başlamıştır. Avrupa Birliği'nin 2024 yılında yürürlüğe giren Siber Esnek-Dayanıklılık Yasası teknoloji üreticilerine bir ürünün yaşam döngüsü boyunca siber güvenliğinin sağlanması sorumluluğunu vererek önemli bir adım atmıştır (European Commission, 2024).

Sonuç: Çoklu Krizler ve Toplum için Siber Esnek-Dayanıklılık

Siber krizlerin farklı fazlarına odaklanmış ve insan-süreç-teknoloji boyutuna dayanan siber esnek-dayanıklılık kavramı sadece organizasyonel uygulamalar olarak düşünülmemelidir. Zira, siber esnek-dayanıklılık kurumlar, bireyler, hükümetler başta olmak üzere tüm toplumsal aktörleri ilgilendirmektedir (Hausken, 2020). Siber güvenlik krizlerinin etkileri tek başlarına sınırlı kalabilse de çoklu krizler çağının da öngördüğü gibi, siber alandaki krizler diğer krizlerle bir araya geldiklerinde tahmin edilemeyen sonuçlar doğabilir. Siber güvenlik sorunları uzun vadede kullanıcıların dijital sistemlere karşı güvenini zedeleyebilir ve teknolojik gelişmelerin benimsenmesinin önü tıkanabilir (Taddeo & Bosco, 2019). Dahası siber krizlerin etkileri organizasyonların boyutlarını aşıp toplumsal ölçekte etkiler doğurabilir. Örneğin, enerji altyapıları gibi kritik varlıkları hedef alan siber saldırılar, yaratacakları fiziksel tahribattan ziyade kamu düzenini bozmak ya da kamu hizmetlerine olan güveni sarsmak bağlamındaki etkileriyle daha zarar verici bir hale gelebilirler (Shandler & Gomez, 2023). Özellikle toplumsal krizlerin yaşandığı doğal afet ve savaş gibi istikrarsız dönemlerde dijital sistemlerdeki zafiyetlerin hedef alınması toplumsal travmaları tetikleyebilir ya da var olan travmaları şiddetlendirebilir (Gandhi vd., 2011). Rusya-Ukrayna savaşında hem kinetik hem siber araçların sivil altyapılarda yarattığı hasarlar siber saldırıların insani boyutlarına ilişkin önemli bulgular sağlamaktadır. Örneğin, Şubat 2022'de Ukrayna sınır karakoluna yapılan HermeticWiper saldırısı kritik verilerin kaybolmasına sebep olmuş ve sığınmacıların Romanya'ya geçişini önemli ölçüde yavaşlatmıştır. Benzer şekilde, Ukrayna vatandaşlarının kişisel bilgilerinin sızdırılması bireylerin doğrudan risk altına girmesine sebep olmuştur (Duguin & Pavlova, 2023).

Sağlık altyapılarını hedef alan siber saldırılar, siber krizlerin somut toplumsal sonuçlarını anlamak için en iyi örneklerden biridir. Örneğin Windows işletim sistemindeki bir zafiyeti kullanan WannaCry fidye yazılımı saldırısı, Birleşik Krallık'ta ambulans ve hasta bakım hizmetlerini etkilemiş, saldırının sonucunda kan test sonuçlarının aktarımı ve aile hekimlerinin hasta dosyalarına ulaşımı kesintiye uğramıştır (NHS, 2023). 2020'de Almanya'nın Düsseldorf şehrinde bir hastanenin bilgisayar sistemlerinin siber saldırı sebebiyle devre dışı kalması bir hastanın başka bir hastaneye nakli esnasında hayatını kaybetmesine neden olmuştur (Tidy, 2020). Bazı çalışmalar siber saldırıların bireylerde anksiyete, öfke ve depresyon gibi olumsuz

duygu durumlarına sebep olabileceğini ön görmektedir (Bada & Nurse, 2020). Siber güvenlik krizlerinin öngörülemez toplumsal ve bireysel boyutlarına, bir sonraki siber güvenlik krizinin nereden ve nasıl geleceğine ilişkin belirsizlikler de eklendiğinde, siber güvenlikteki işlevselliği muhafaza etmek, zararları azaltmak, krizlerden öğrenmek ve yeni koşullara uyum sağlayabilmeyi hedefleyen siber esnek-dayanıklılık kavramı öne çıkmaktadır.

Bununla beraber, siber esnek-dayanıklılık kavramının sihirli bir reçete olmadığı hatta zaman zaman ikircikli hususlar yaratabildiği de göz ardı edilmemelidir. Örneğin, esnek-dayanıklılık kavramı özellikle kriz dönemlerinde ortaya çıkan sorumluluk boşluğunu doğurabilecek neo-liberal bir yönetişim biçimi olarak sunulmaktadır (Bourbeau, 2015). Diğer deyişle, belirsizliklere karşı esnek-dayanıklılık gereksinimi anlatısı daha önce kamuya ait olan "güvenliğin sağlanması" sorumluluk alanından devletin görece çekilebilmesine ve sorumluluğun farklı aktörler arasında dağıtılmasına fırsat vermektedir. Konuyu siber güvenlik özelinde incelediğimizde, özellikle kritik altyapıların ya da hassas verilerin özel sektör eliyle işletiliyor olması "*siber güvenliği kim sağlamalı*" sorusunu da beraberinde getirmiş ve siber güvenlik alanı sorumluluk karmaşası ile karşı karşıya kalmıştır. Ek olarak siber saldırıların özellikle son kullanıcıları sıklıkla hedef alması siber riskleri orantısız şekilde bireyselleştirmiş ve bireyleri adeta siber tehditler karşısında yalnız bırakmıştır (Renaud vd., 2018, 2020).

Özetle, kamu, özel sektör ve bireylerin işbirliğini gerektiren siber esnek-dayanıklılık belirsizliğe çare olarak sunulmuş; ancak bu işbirliğinin derinliği ve çerçevesi net olarak çizilememiştir. Öte yandan farklı aktörler arasında güven inşasının siber esnek-dayanıklılık kapasitesini arttırdığı göz önüne alınmalıdır. Yönetmelikleri inşa eden düzenleyiciler ile işletmeciler ve çalışanları arasındaki ilişkide bütün paydaşların sorumluluğu eşit şekilde üstlenmesi gerektiğinin de altı çizilmelidir. Sorun, kimin hatalı olduğundan ziyade, krizi aşmak için nasıl birlikte çalışılacağı ve hangi şekilde hızlı bir çözüme ulaşılarak sistemin çalışır hale getirilebileceğidir.

Çoklu krizler çağında siber risklerin toplumsal etkilerinin bertaraf edilebilmesi ve sürdürülebilir bir siber esnek-dayanıklılık siber güvenlik alanında *erişilebilir, yenilikçi, sorumlu* ve *kapsayıcı* politikaları benimsemekle mümkündür. Öncelikle erişilebilir siber güvenlik, toplumdaki tüm aktörlerin ihtiyaçlarına cevap verebilen siber güvenlik politikaları hayata geçirmektir. Siber güvenliğe erişimde aslında çok konuşulmayan bir eşitsizlik söz konusudur. Bir başka deyişle toplumun özellikle risk altındaki kesimlerinin güvenlik ve gizlilik hizmetlerine erişimlerinde sosyo-ekonomik faktörler ya da dijital okuryazarlık gibi nedenlere dayanan bariyerler bulunmaktadır (Renaud & Coles-Kemp, 2022). Siber güvenlik hizmetlerine erişimdeki eşitsizlikler sadece bireyler arasında değil ülkeler ve kurumlar arasında da önemli bir sorundur. Öte yandan bağımlılık içerisinde bulunan sistemlerde sadece faydanın değil zafiyetlerin de paylaşılmasından dolayı sistemin herhangi noktasında gelişen bir güvenlik sorununun tüm sistemi etkileyecek yani sistemsel bir risk yaratma potansiyeli bulunmaktadır.

Gelişen teknolojiler siber güvenlik için hem bir fırsat hem de risk teşkil etmekte yani hem saldırganlar hem de siber güvenlik uzmanları tarafından kullanılabilmektedir. Tehdit aktörleri ve kullandıkları yöntemlerin de hızlı değişimi yenilikçi bir siber güvenlik anlayışı ge-

reksinimi de beraberinde getirmektedir. Sorumlu siber güvenlik anlayışı, siber güvenliğe ilişkin risklerin azaltılması görevini aktörlerin sağladığı fayda ve kapasitelerine istinaden dağıtmaktır. Örneğin kamu otoriteleri, üreticilerin, tedarikçilerin ya da teknoloji geliştiricilerin takip etmeleri gereken asgari süreçleri belirlerken, özel sektörün bu standartları takip etmesi ve yaşanan siber olayları bildirmek gibi sorumlulukları yerine getirmesi beklenmektedir (Taddeo & Bosco, 2019).

Kapsayıcı siber güvenliği ise hem toplumun cinsiyet, etnik grup ya da yaş grupları bağlamında farklı kesimlerinin siber güvenlik ihtiyaçlarını gözetmek hem de siber güvenlik alanında çalışan işgücünü, özellikle cinsiyet eşitliği bağlamında, çeşitlendirmek olarak düşünebiliriz. Öncelikle nasıl ki siber güvenlik hizmetlerine erişim konusunda adaletsizlikler söz konusuysa, siber saldırıların özellikle toplumun daha kırılgan kesimlerini daha şiddetli şekilde etkilediğinden bahsetmek mümkündür. Bu çerçevede, bu etkilerin derinlemesine tartışılabileceği ulusal veya uluslararası platformların varlığı ve farklı kesimleri temsil edebilen sivil toplum örgütlerinin politika yapım süreçlerine katılımının desteklenmesi önemlidir (Emerson-Keeler vd., 2023; Hofstetter & Pourmalek, 2023).

Siber güvenlikteki iş gücünde çeşitliliği sağlamadan yeni tehdit ve belirsizliklerle mücadele oldukça zorlayıcı olacaktır. Siber güvenlik sektörünün bu hususta aşması gereken en önemli bariyerlerden birisi kadınların siber güvenlik sektörüne katılımının görece az olması ve bu bağlamda derinleşen yetenek krizidir. Unutmamak gerekir ki, tehditlerin dinamik olduğu siber güvenlik dünyasında yaratıcı ve çok yönlü düşünebilen, farklı sesleri dile getirebilen ve çeşitlilikleri yansıtabilen bir iş gücü en önemli gereksinimlerden biri olarak karşımıza çıkmaktadır. Son olarak, siber esnek-dayanıklılığın tehditlerin sürekli gelişmesine paralel olarak daimi olarak gelişen, yeni teknik ve taktik unsurlarla desteklenmesi gereken bir süreç olması gerektiği göz ardı edilmemeli, bütün paydaşların bu sürece katılmasının elzem olduğunun da altı çizilmelidir.

1 Siber Esnek-Dayanıklılık Mühendisliği Çerçevesi siber esnek-dayanıklılığın dört amacının yanında, sekiz hedefini ve bunlara ulaşmak için on dört tekniği ortaya koyar. Bu sekiz hedef "Anlamak, Hazırlanmak, Önlemek /Kaçınmak, Devam Ettirmek, Sınırlandırmak, Yeniden Yapılandırmak, Dönüştürmek, Yeniden Mimari Oluşturmak'tır. On dört teknik ise "Uyarlanabilir Yanıt, Analitik İzleme, Aldatma, Öngörülemezlik, Çeşitlilik, Dinamik Konumlandırma, Kalıcı Olmama, Ayrıcalık Kısıtlaması, Bölümlendirme / İzolasyon, Koordine Savunma, Dinamik Temsil, Yeniden Hizalama, Yedeklilik, Doğrulanmış Bütünlük" olarak verilmiştir. Bu çalışmada bu hedef ve teknikler gözden geçirilmiş ve sosyo-teknik katmanlar içinde yeniden değerlendirilmiştir.

Kaynakça

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62-68. https://doi.org/10.1109/TALE.2018.8615162.

ANSSI. (2022). *Anticipating and Managing Your Cyber Crises Communication*. The French National Cyber Security Agency (ANSSI).

Aoyama, T., Sato, A., Lisi, G., & Watanabe, K. (2020). On the Importance of Agility, Transparency, and Positive Reinforcement in Cyber Incident Crisis Communication. Içinde S. Nadjm-Tehrani (Ed.), *Critical Information Infrastructures Security* (C. 11777, ss. 163-168). Springer International Publishing. https://doi.org/10.1007/978-3-030-37670-3_13.

Aradau, C. (2014). The promise of security: Resilience, surprise and epistemic politics. *Resilience*, *2*(2), 73-87. https://doi.org/10.1080/21693293.2014.914765

Bada, M., & Nurse, J. R. C. (2020). Chapter 4—The social and psychological impact of cyberattacks. İçinde V. Benson & J. Mcalaney (Ed.), *Emerging Cyber Threats and Cognitive Vulnerabilities* (ss. 73-92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *Guide for cybersecurity event recovery* (No. NIST SP 800-184; s. NIST SP 800-184). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184

BBC. (2016, Şubat 26). *Hackers behind Ukraine power cuts, says US report*. https://www.bbc.com/news/technology-35667989.

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A Review of Colonial Pipeline Ransomware Attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8-15. https://doi.org/10.1109/CCGridW59191.2023.00017.

Bıçakcı, S., & Gücüyener Evren, A. (2023). Responding cyber-attacks and managing cyber security crises in critical infrastructures: A sociotechnical perspective. İçinde *Management and Engineering of Critical Infrastructures—1st Edition*. Elsevier. https://shop.elsevier.com/books/management-and-engineering-of-critical-infrastructures/tekinerdogan/978-0-323-99330-2.

Bıçakcı, S. (2024, Temmuz 24). *Dijital distopya: Mavi ekran, siber tehditler ve esnek-dayanıklılık - Fikir Turu*. https://fikirturu.com/toplum/dijital-distopya-mavi-ekran-siber-tehditler/.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. Içinde A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Ed.), *New Contributions in Information Systems and Technologies* (ss. 311-316). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31.

Bodeau, D., Graubart, R., Heinbockel, W., & Laderman, E. (2015). *Cyber Resiliency Engineering Aid—The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*. https://www.mitre.org/news-insights/publication/cyber-resiliency-engineering-aid-updated-cyber-resiliency-engineering.

Boin, A., & Hart, P. (2022). From crisis to reform? Exploring three post-COVID pathways. *Policy and Society*, *41*(1), 13-24. https://doi.org/10.1093/polsoc/puab007.

Bonime-Blanc, A., & Saban, T. (2021, Eylül 27). *The 5 "Ts" of cyber-crisis readiness for any kind of organization.* World Economic Forum. https://www.weforum.org/stories/2021/09/cybersecurity-cyber-crisis-readiness/

Bourbeau, P. (2015). Resilience and International Politics: Premises, Debates, Agenda. *International Studies Review*, *17*(3), 374-395. https://www.jstor.org/stable/24758620.

Brantly, A. F. (2021). Risk and uncertainty can be analyzed in cyberspace. *Journal of Cybersecurity*, *7*(1), tyab001. https://doi.org/10.1093/cybsec/tyab001.

Briggs, B. (2019). *Hackers hit Norsk Hydro with ransomware. The company responded with transparency*. Source. https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/.

Center for Internet Security. (2024). *What is an ISAC?* CIS. https://www.cisecurity.org/isac/.

Chatterjee, R., & Hepfer, M. (2023). *Creating Cyber Resilience By Routine*. ISTARI. https://istari-global.com/insights/perspectives/creating-cyber-resilience-by-routine/.

Christine, D. I., & Thinyane, M. (2022). Socio-technical Cyber Resilience: A Systematic Review of Cyber Resilience Management Frameworks. Içinde J. Marx Gómez & M. R. Lorini (Ed.), *Digital Transformation for Sustainability: ICT-supported Environmental Socio-economic Development* (ss. 573-597). Springer International Publishing. https://doi.org/10.1007/978-3-031-15420-1_28.

Duguin, S., & Pavlova, P. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594.

Dunn Cavelty, M., Kaufmann, M., & Søby Kristensen, K. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*, *46*(1), 3-14. https://doi.org/10.1177/0967010614559637.

Emerson-Keeler, R., Swali, A., & Naylor, E. (2023). *Integrating gender in cybercrime capacity-building*. Chatham House. 10.55317/9781784135515.

ENISA. (2024). *Best practices for cyber crisis management: February 2024*. European Union Agency for Cybersecurity (ENISA). https://data.europa.eu/doi/10.2824/767828.

ESET. (2024). *Why Employee Mistakes Are The Biggest Cybersecurity Threat*. ESET. https://www.eset.com/za/about/newsroom/press-releases-za/press-releases/why-employee-mistakes-are-the-biggest-cybersecurity-threat/.

European Commission. (2024). *Cyber Resilience Act | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Forêt, C. (2023). *Building a Crisis Response Team: Key Roles, Benefits, and Setup for Cybersecurity*. https://www.c-risk.com/blog/crisis-response-team.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, *30*(1), 28-38. IEEE Technology and Society Magazine. https://doi.org/10.1109/MTS.2011.940293.

Golandsky, Y. (2016). Cyber crisis management, survival or extinction? *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, 1-4. https://doi.org/10.1109/CyberSA.2016.7503291.

Greiman, V. (2023). Known Unknowns: The Inevitability of Cyber Attacks. *Proceedings of the 22nd European Conference on Cyber Warfare and Security*, *22*, Article 1. https://doi.org/10.34190/eccws.22.1.1316

Gryszkiewicz, A., & Chen, F. (2012). Temporal aspects in crisis management and its implications on interface design for situation awareness. *Cognition, Technology & Work (Online)*, *14*(2), 169-182. https://doi.org/10.1007/s10111-011-0199-y.

Hadley, J. (2023). *From Awareness To Resilience: The Evolution Of People-Centric Cybersecurity*. Forbes. https://www.forbes.com/sites/jameshadley/2023/11/29/from-awareness-to-resilience-the-evolution-of-people-centric-cybersecurity/.

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204.

Hofstetter, J.-S., & Pourmalek, P. (2023). *Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-level Approaches to Cybersecurity*. Global Network of Women Peacebuilders (GNWP). https://ict4peace.org/wp-content/uploads/2023/03/Gendering-Cybersecurity-through-WPS-Final-Report_March-2023.pdf.

Hussain, A., Kuhn, K., & Shaikh, S. A. (2020). Games for Cybersecurity Decision-Making. Içinde X. Fang (Ed.), *HCI in Games* (C. 12211, ss. 411-423). Springer International Publishing. https://doi.org/10.1007/978-3-030-50164-8_30.

ISACA. (2024). *State of Cybersecurity 2024*. ISACA. https://www.isaca.org/resources/reports/state-of-cybersecurity-2024?tfa_next=%2Fresponses%2Flast_success%3Fjsid%3DeyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ImZlNzZkMWZkYzQ5Y2Q0ZTQ0NGRjMTQ3ZWUxNmUyMjcyIg.1vXTWv4UAed7FcqOz1PPq3qJh7ikdD0XXB5bm0-ekJA.

ISC2. (2024). *2024 ISC2 Cybersecurity Workforce Study*. ISC2. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study.

Juntunen, T., & Virta, S. (2019). Security Dynamics: Multilayered Security Governance in an Age of Complexity, Uncertainty, and Resilience. İçinde *Leading Change in a Complex World: Transdisciplinary Perspectives* (ss. 67-84). Tampere University Press.

Kaschner, H. (2022). *Cyber Crisis Management: The Practical Handbook on Crisis Management and Crisis Communication*. Springer Nature.

Kazemi, A. (2023). *European AI Alliance—AI for Crisis Management: Impacts, Challenges, Best Practices*. Futurium. https://futurium.ec.europa.eu/en/european-ai-alliance/forum-discussion/ai-crisis-management-impacts-challenges-best-practices.

Kaziukonis, V. (2024). *Council Post: How To Build A Culture Of Cyber Resilience In Your Organization*. Forbes. https://www.forbes.com/councils/forbestechcouncil/2024/09/05/how-to-build-a-culture-of-cyber-resilience-in-your-organization/.

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 102036. https://doi.org/10.1016/j.cose.2020.102036.

Kott, A., & Linkov, I. (2021). To Improve Cyber Resilience, Measure It. *Computer*, *54*(2), 80-85. Computer. https://doi.org/10.1109/MC.2020.3038411.

Llansó, T. H., Hedgecock, D. A., & Pendergrass, J. A. (2021). The State of Cyber Resilience: Now and in the Future. *Johns Hopkins APL Technical Digest*, *35*(4).

Morgan, S. (2018, Temmuz 19). Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion. *Cybercrime Magazine*. https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/.

National Institute of Standards and Technology. (2024). *Cyber Resiliency*. https://csrc.nist.gov/glossary/term/cyber_resiliency

NHS. (2023). *NHS England business continuity management toolkit case study: WannaCry attack*. https://www.england.nhs.uk/long-read/case-study-wannacry-attack/.

Onwubiko, C. (2020). Focusing on the Recovery Aspects of Cyber Resilience. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1-13. https://doi.org/10.1109/CyberSA49311.2020.9139685

Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity*, *4*(1), 8. https://doi.org/10.1186/s42400-021-00071-z.

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2024). "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents. *Computers & Security*, *139*, 103699. https://doi.org/10.1016/j.cose.2023.103699.

Pearlson, K. (2024). *When Cyberattacks Are Inevitable, Focus on Cyber Resilience*. https://hbr.org/2024/07/when-cyberattacks-are-inevitable-focus-on-cyber-resilience.

Pearlson, K., & Miller, K. (2024, Eylül 16). *How to Build a Cyber Crisis Communications Plan*. MIT Sloan Management Review. https://sloanreview.mit.edu/article/how-to-build-a-cyber-crisis-communications-plan/.

Petrosyan, K. (2021, Mayıs 11). *Colonial pipeline outage in the United States underscores risks to energy supplies – Analysis*. IEA. https://www.iea.org/commentaries/colonial-pipeline-outage-in-the-united-states-underscores-risks-to-energy-supplies.

Ransbotham, S., Fichman, R. G., Gopal, R., & Gupta, A. (2016). Special Section Introduction: Ubiquitous IT and Digital Vulnerabilities. *Information Systems Research*, *27*(4), 834-847. https://www.jstor.org/stable/26652532.

Rapoport, M., & Andriotis, A. (2017, Ekim 28). States Push Equifax to Explain Why It Took 6 Weeks to Disclose Hack. *Wall Street Journal*. https://www.wsj.com/articles/states-push-equifax-to-explain-why-it-took-6-weeks-to-disclose-hack-1509196933.

Renaud, K., & Coles-Kemp, L. (2022). Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge. *SN Computer Science*, *3*(5), 346. https://doi.org/10.1007/s42979-022-01239-1.

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security*, *78*, 198-211. https://doi.org/10.1016/j.cose.2018.06.006.

Renaud, K., Orgeron, C., Warkentin, M., & French, P. E. (2020). Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. *Public Administration Review*, *80*(4), 577-589. https://doi.org/10.1111/puar.13210.

Renckens, P., Ferentinos, L., & Wielart, A. (2024). *Never Waste a Good Crisis: The Six Success Factors of Cyber Resilience*.

Riley, T. (2021, Haziran 8). Colonial Pipeline CEO says company didn't have plan for potential ransomware attack. *CyberScoop*. https://cyberscoop.com/colonial-pipeline-ransomware-senate-hack/.

Salviotti, G., & Abbatemarco, N. (2023). Understanding the Role of Leadership Competencies in Cyber Crisis Management: A Case Study. *Proceedings of the 56th Hawaii International Conference on System Sciences*, 6068-6077.

Savić, S., & Krivokapić, J. (2022). *Booklet on Crisis Communication*. Geneva Centre for Security Sector Governance. https://www.dcaf.ch/sites/default/files/publications/documents/BookletCrisisCommunication_EN_web_Jan2023.pdf.

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the Five Hard Problems of Cybersecurity. *Risk Analysis*, *39*(10), 2119-2126. https://doi.org/10.1111/risa.13309.

Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, *20*(4), 359-374. https://doi.org/10.1080/19331681.2022.2112796.

Sophos. (2024). *The Future of Cybersecurity in Asia Pacific and Japan*. Sophos. https://assets.sophos.com/X24WTUEQ/at/wkk9cs4q3f7rg52hj33t/sophos-future-of-cybersecurity-apj-wp.pdf.

Statista. (2024). *IoT connections worldwide 2022-2033*. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Taddeo, M., & Bosco, F. (2019, Ağustos 22). *We must treat cybersecurity as a public good. Here's why*. World Economic Forum. https://www.weforum.org/stories/2019/08/we-must-treat-cybersecurity-like-public-good/.

TechTarget. (2022). *Cisco hacked by access broker with Lapsus$ ties*. Search Security. https://www.techtarget.com/searchsecurity/news/252523746/Cisco-hacked-by-access-broker-with-Lapsus-ties.

Tidy, J. (2020, Eylül 18). *Police launch homicide inquiry after German hospital hack*. https://www.bbc.com/news/technology-54204356.

Tonkin, A., Kosasih, W., Grobler, M., & Nasim, M. (2023). Simulating cyber security management: A gamified approach to executive decision making. *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, 1-8. https://doi.org/10.1145/3551349.3561148.

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695-1719. https://doi.org/10.1007/s10207-023-00811-x.

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. World Economic Forum.