HAKEMLİ Denetişim
Ortak Aklın Harmanı
Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 13, Sayı: 26, 44-51, 2022

Teorik Makale

MEZENFORMASYON VE DEZENFORMASYON FAALİYETLERİ, SEKTÖREL RİSKLER VE İLETİŞİM TEKNOLOJİLERİ

(MISINFORMATION AND DISINFORMATION ACTIVITIES, SECTORAL RISKS AND COMMUNICATION TECHNOLOGIES)

Dr. Nurat KARA[*],

ÖZ

Bilgi bozukluğu iletişim teknolojilerinin yaygınlaşması ile ulusal ve uluslararası bir sorun olma yolunda ilerlemektedir. Teknolojilerin hızla gelişmesi, yaşanan sosyo-ekonomik olaylar ve küresel sağlık problemleri gibi konular ekseninde bilgi bozukluğu sürekli önemi artan bir konu olarak karşımıza çıkmaktadır. Genellikle mezenformasyon veya dezenformasyon olarak detaylandırılan bilgi bozukluğu toplumları etkilediği gibi kamu ve özel sektörü de etkisi altına almaya başlamıştır. Hem dezenformasyon, yani kasıtlı yanıltma, hem de mezenformasyon, yani farkında olmadan bilgi bozukluğuna sebebiyet verme, toplumları ve sektörleri yeni bir takım siber tehditlerle karşı karşıya bırakmaktadır. Bu durum bazı, yeni ve ciddiye alınması gereken sektörel riskleri de beraberinde getirmektedir. Bazı sektörel risklerle birlikte, yeni iletişim olanaklarının hızla çeşitlenmesi dijitalleşmeyi ve siber tehditleri de yaygınlaştırmaktadır. Dijital dönüşüm bir yandan sektörler için bazı yeni olanakları yaratsa da meydana getireceği muhtemel siber sorunların şimdiden dikkate alınması önemli bir çalışma alanı olarak düşünülmektedir. Aksi durumun ileride önemli birtakım olumsuz sonuçları beraberinde getirmesi olasıdır. Bu çalışma ile bilgi bozukluğunun, hem dezenformasyon hem de mezenformasyon, sektörel olarak yaratacağı riskleri anlamak ve de bu risklere yönelik birtakım önerileri sunmak amaçlanmaktadır. Çalışmada bu öneriler şu şekilde sıralanmıştır: Dijital dönüşüm stratejileri oluşturmak, siber riskleri belirlemek ve değerlendirmek, standartlar ve normlar belirlemek ve benimsemek. Bunun yanı sıra, mezenformasyon ve dezenformasyonu önlemek için çeşitli endüstriler, kamu ve özel sektör, uluslararası liderler ve siyasi liderlere fayda sağlayabilecek ortaklıklarla yatırımları artırmak önem arz etmektedir. İşbirliği içerisinde olacak olan bu aktörler yeni iletişim teknolojilerinin alt yapısına yapacakları yatırımlarla ve kurulacak ortak sistemlerle küresel boyutta dezenformasyon ve mezenformayson ile mücadale edebilirler.

Anahtar Kelimeler: Bilgi Bozukluğu, Sektörel Tehditler, Siber Güvenlik, İletişim Teknolojileri, Dezenformasyon

Jel Kodları: M, O3

ABSTRACT

Information disorder is on its way to becoming a national and international problem with the spread of communication technologies. Information disorder is a constantly increasing issue in the axis of issues such as the rapid development of technologies, socio-economic events, and global health problems. Information disorder, often detailed as misinformation or disinformation, has begun to affect the sectors and societies. Both disinformation, that is, deliberate deception, and misinformation, causing information corruption without being aware of it, expose societies and sectors to a new set of cyber threats. This situation brings some new and sectoral risks that should be taken seriously. Along with some sectoral risks, the rapid diversification of new communication opportunities makes digitalization and cyber threats widespread. Although digital transformation creates some new opportunities for the sectors, it is considered an essential field of study to consider the possible cyber problems it will create. Otherwise, it may bring some essential negative consequences in the future. This study aims to understand the risks that information disorder will create both disinformation and misinformation sectoral and present

• Dr., Bilgi İşlem Daire Başkanı, Hatay Mustafa Kemal Üniversitesi, 0000-0001-9753-1593, nkara@mku.edu.tr

some suggestions for these risks. In the study, these recommendations are listed as follows: Creating digital transformation strategies, identifying, and evaluating cyber risks, setting and adopting standards and norms, preventing misinformation and disinformation, and ***increasing investments with various industries, sectors, and international leaders and partnerships that can benefit leaders.***

Keywords: *Information Distortion, Sectoral Threats, Cyber Security, Communication Technologies, Disinformation*

JEL Classification: *M, O3*

1. GİRİŞ

Yeni bir bilgi çağının içindeyiz; eski teknolojilerin yeni teknolojilere evirildiği ve bilgi teknolojilerine dayanan üçüncü sanayi devriminden sonrasını tecrübe etmekteyiz. Dördüncü sanayi devrimi, pek çok zaten hayatımızda olan teknolojinin olgunlaşması akabinde bir araya gelmesinden meydana gelmektedir. Artan insan kaynakları maliyetleri ve diğer başka sebepler teknoloji tabanlı yeni sistemlerin kurulmasını gerekli kılmıştır. Dolayısıyla ilk üç devrimin ötesinde üretim süreçlerinde insansızlaşmaya gidilen dördüncü sanayi devriminden bahsedilmektedir. Dördüncü sanayi devrimi ile birlikte hem kamu hem de özel sektörlerde, toplumsal bir değişim yaşanmakta ve değişimle birlikte yeni birtakım riskleri de konuşur hale gelmekteyiz (Schwab, 2017). Kaplan ve Haenlein' göre ise (2019, s. 679), dijital dönüşüm, dijital teknolojilerin toplumu tüm alanlarda entegre ederek ve büyük ölçekte değişimlere maruz bırakmaktadır. Bu değişime dijital dönüşüm denilmektedir. Dijital dönüşüm bir yandan toplumları değiştirirken diğer taraftan hükümetleri ve kamu yönetimini de etkisi altına almaktadır (Kaplan ve Haenlein, 2019). Bu dönüşümün küresel olarak her sektöre etkisi bulunmakta ve bu etki değişimi zorunlu kılmaktadır (Schwab, 2017). Hem kamu hem özel sektörün bu değişim sebebi ile çok zorlanacağı bir gerçektir (Saarikko et al., 2020). Dijitalleştirilmiş bilgi, ürün ve hizmetlerin yanı sıra dijital ve fiziksel bileşenleri entegre eden sistemlerin ve sektörlerin ayrılmaz bir parçası haline gelmektedir (Saarikko et al., 2020). Kamu ve özel sektörün kullandığı ve oluşturduğu bilgi ve bu bilgiyi işlemek için kullanılan geniş teknoloji yelpazesi endüstrileri dönüştürebilir, sektörler için rekabet avantajlarını yeniden şekillendirebilir ve yeniliği yönlendirebilir durumdadır (Porter ve Millar, 1985). Kaliteli bilgi edinme, sektörel bazda dönüşüm, performans ve sürdürülebilir olmak yeni mücadele alanları olarak görülmektedir.

Öte yandan bilgi bozukluğu, genellikle, mezenformasyon ve dezenformasyon olarak değerlendirilir. Bu bir süredir önemli bir endişe kaynağı olsa da siber saldırıların sıklığı ve karmaşıklığındaki sürekli artış, seçim sürecinde ortaya çıkan bilgi kirliliği COVID-19 sırasında ortaya çıkan bilgi bozukluğu gibi krizler, bu durumu sektörler için bir soruna dönüştürdü. Bilgi bozukluğu, kuruluşlar için önemli tehditler ve riskler oluşturur. Dünya Ekonomik Forumu'nun 2013 Küresel Risk Raporu, dijital bilgi bozukluğu riskinin altını çizmektedir. Dijital dezenformasyon riski daha sonra 2016 ABD başkanlık seçimlerinde ve COVID-19 krizi boyunca geniş çapta tanındı. Bu vakalarda bilgi bozukluğunun etkisi önemli olmuştur. Bu bağlamda çalışma hem dezeneformasyon hem de mezenformasyonun sektörel olarak yaratacağı riskleri anlamak ve bu risklere karşı alınabilecek tedbirleri sunmayı amaçlamaktadır. Buradan hareketle çalışma dezeneformasyon ve mezenformasyona karşı dijital dönüşüm stratejileri oluşturmayı, siber riskleri belirlemeyi ve değerlendirmeyi, belirli standartlar ve normlar oluşturmayı ve benimsemeyi önermektedir. Bunun yanı sıra mezenformasyon ve dezenformasyonu önlemek için çeşitli endüstriler, sektörler, uluslararası liderler ve liderlere fayda sağlayabilecek ortaklıklarla yatırımları arttırmak önem arz etmektedir.

2. BİLGİ BOZUKLUĞU: MEZENFORMASYON VE DEZENFORMASYON

Öncelikle bilgi bozukluğunu anlamak için, dezenformasyon ve mezenformasyonun ne anlama geldiğini tanımlamak ve netleştirmek gerekmektedir. Mezenformasyon çok geniş kapsamlı olarak yanlış bilgiyi ve bilgi bozukluğunu ifade etmek için kullanılmıştır (Oxford İngilizce Sözlüğü 2020). Mezenformasyon, mevcut durumda, manipülatif veya kötü niyetli olunmadan oluşturulmuş veya paylaşılan yanıltıcı bilgileri tanımlamak için kullanılmaktadır (Ireton ve Posetti, 2018). Dezenformasyon, resmî kurumlar tarafından yabancı bir güce veya medyaya, alıcının politikasını veya görüşünü etkilemek amacıyla sağlananlar da dahil olmak üzere, kasıtlı olarak yanlış bilgilerin yayılması olarak tanımlanmaktadır (Oxford İngilizce Sözlüğü, 2020).

Birleşmiş Milletler, dezenformasyonu, insanlara dürüst olmayan bilgiler sağlayarak insanları şaşırtmaya veya manipüle etmeye yönelik kasıtlı, genellikle düzenlenmiş girişimler olarak tanımlar. Avrupa Komisyonuna göre (2018) dezenformasyon, yanlış veya yanıltıcı olabilecek her türlü bilgi olarak ele alınmaktadır. Yanı sıra komisyon, dezenformasyon sonucu risklerin yalnızca siyasi alanlarda veya kültürel değerlerde yozlaşma gibi gerçekleşmeyeceğini nihayetinde sağlık ve finans sektörlerini de içine alan daha geniş bir alanda zararlı olacağını ifade etmektedir. Dezenformasyonu, ekonomik kazanç sağlamak veya kasıtlı olarak kamuoyunu yanıltmak amacıyla, kamuoyuna zarar verebilecek, doğrulanabilir yanlış veya yanıltıcı bilgilerin oluşturulması, sunulması ve yayılması olarak tanımlamaktadır (Avrupa Sayıştayı, 2020). Dezenformasyon, ABD Dışişleri

Bakanlığı'na göre (Nemr & Gangware, 2019), diğer dezenformasyon tanımlarıyla büyük ölçüde tutarlı olan, yanlış yönlendirme veya zarar verme amaçlı yanlış bilgilerin kasıtlı olarak yayılması olarak geniş çapta tanımlanmaktadır.

Sahte haber, yanlış, uydurma veya kasıtlı olarak yanıltıcı bilgi ileten veya içeren veya bu şekilde nitelendirilen veya okunan haberler olarak tanımlanmaktadır (Oxford İngilizce Sözlüğü, 2020). ABD başkanlık seçimleri terimin popülerlik kazanmasında önemli bir rol sahibidir (NATO, 2020). Sahte haber, iki ana şekilde kullanılmaktadır: Özellikle belirli bir siyasi veya ideolojik amaca hizmet eden, sosyal medyada ve internette dolaşan yanlış haberlere atıfta bulunmak veya taraflı, güvenilmez olarak görülen medya raporlarını itibarsızlaştırmaya çalışmak (Oxford İngilizce Sözlüğü, 2020). Bu tanımlardan bazıları dezenformasyonla örtüşmektedir.

3. SEKTÖREL TEHDİTLER VE İLETİŞİM TEKNOLOJİLERİ

Birçok siber saldırı türü yanıltıcı bilgiler kullanmaktadır. Sosyal mühendislik, sektörlere yönelik en yaygın siber saldırı türüdür (ISACA, 2020). İletişim teknolojilerinin artan kullanımı, sosyal mühendislik tekniklerinde bir artışa yol açmıştır, öyle ki günümüzde çoğu siber saldırı bir tür sosyal mühendislik içermektedir (ENISA, 2020). Sosyal mühendislik teknikleri arasında bahane, yemleme, karşılıksız bırakma, bekleme hattı, sırasını bekleyen ile kimlik avı ve hedefli kimlik avı yer alır (ENISA, 2020). Kimlik avı veya dolandırıcılık amaçlı iletişimler göndermek, giderek yaygınlaşan bir siber tehdittir (Cisco, 2020). Bu nedenle, tanım gereği, kimlik avı yanıltıcı bilgiler kullanır. Kimlik avı, özellikle sektörler için en güçlü tehditlerden biridir ve başlı başına bir sektör haline gelmiştir (Boddy, 2018). Sektörlere yönelik sürekli ve yaygın bir saldırı türüdür, büyük olasılıkla tüm sektörlerde günlük veya saatlik olarak gerçekleşebilmektedir ve sektörlerin yüzde 77'si en az ayda bir kimlik avı saldırısı tecrübe etmiştir (Boddy, 2018, s. 9). 2020'deki banka havalesi üzerinden gerçekleşen siber saldırılar 80 bin 183 dolara mal olmuş ve ülkeler arası ortalama 1,27 milyon dolar zarara sebebiyet verebilecek şekilde sektörleri hedef aldığı bilinmektedir (APWG, 2020).

İletişim teknolojilerinin yaygınlaşması ile pek çok sektör ve kurum iş yapış şeklini değiştirmek zorunda kalmıştır. Giderek kullanımı artan teknolojiler eskiden kas gücü ile yapılan işleri devralmıştır. Bu durum giderek artan bir büyüklükte olan kamu ve özel sektörleri dijitalleştirirken, bu denli büyük bir bilgisayar tabanlı hale gelmenin bir sonucu olarak, sektörler siber risklere karşı daha açık hale gelmiştir. Tüm bilgilerin, gizli evrakların, rekabetle ilgili hassas içeriklerin sızdırılması, çalınması, bozulması mümkün hale gelmiştir. Siber saldırı denildiğinde en yaygın türlerinden biri de sosyal mühendisliktir. Sosyal mühendislik türünde gerçekleşen siber saldırılar %15 iken, gelişmiş kalıcı tehdit (APT- Advanced Persistent Threats) olarak tanımlanan saldırı türleri ise %10 olarak gerçekleşmektedir (ISACA, 2020). Gelişmiş kalıcı tehditler yüksek düzeyde uzmanlık ve önemli kaynaklar gerektirir. Kurumların misyonları, iş fonksiyonları ve bilgi sistemlerini bozmak, zarar vermek amaçlı pek çok aldatma saldırısı veya diğer türlü çoklu saldırı yöntemleri kullanılmaktadır (NIST, 2015).

Gelişmiş kalıcı tehditler dezenformasyon, açık eylemler, gizli siber operasyonlar (yani sosyal mühendislik) ve bir dizi aktör kullanılarak gerçekleşebilmektedir. Siber Tehdit Aktörleri kurumlar üzerinde çeşitli ve kritik etkilere sahip olabilmekte ve önelem alınmazsa kurumları derinden tehdit edebilmektedir. Siber suçlular %22 oranı ile en büyük istismarcılar olmaya devam etmekte ve genellikle kimlik avı yöntemi kullanarak saldırılarını gerçekleştirmektedir (ISACA, 2020). Bir diğer dikkate değer aktör kategorisi de %9 ile ulus/devlet olarak bilinmektedir (ISACA, 2020). Bu yüzde nispeten küçük görünse de ulusal/hükümet siber saldırıları kuruluşlar üzerinde yıkıcı bir etkiye sahip olabilir. Aynı zamanda, sektörlerin büyük çoğunluğunun bu kadar sofistike ve zengin oyunculardan korunamaması da muhtemeldir. Ek olarak, ulus devletler suç grupları, içeriden öğrenenler ve diğer bilgisayar korsanları gibi diğer Siber Tehdit Aktörleri kullanarak siber tehditlerini artırabilir. Siber açıdan yarattığı tehditler açısından düşünüldüğünde ulus devletler ve gelişmiş kalıcı tehditler birbirinin yerine kullanılmıştır (CIS, 2021).

COVID-19 salgını, sektörel tehditleri ve siber güvenlik algısını kökten değiştirdi. Sadece mevcut riskleri artırmakla kalmadı, aynı zamanda yeni tehditler de yarattı. Uzaktan çalışma teknolojilerinin geniş çapta benimsenmesi, müşteriye yönelik ağlarda artan etkinlik ve pandemiye yanıt olarak çevrimiçi hizmetlerin daha yaygın kullanımı siber riskleri artırdı (ICC, 2020). Tüm bu faktörler, sektörler ve müşteriler için saldırı yüzeyini ve siber riskleri artırdı. COVID-19, sektörlerin yanı sıra hükümetlere, kritik altyapılara ve evlere yönelik siber saldırıları körüklemekte ve saldırılar daha karmaşık, hedefli, yaygın ve tespit edilemeyen hale getirmiştir (ENISA, 2020). Bir Interpol (2020) değerlendirmesine göre, COVID-19'un siber suç üzerindeki etkisi, küçük sektörlerden büyük sektörlere, hükümetlere ve kritik altyapıya doğru bir geçiş içinde olduğunu aktarılmaktadır. Aynı zamanda, mikro, küçük ve orta ölçekli sektörler ve çalışanları ile girişimciler ve serbest meslek sahipleri en çok etkilenenler arasında yer almaktadır (ICC, 2020). Mezenformasyon ve dezenformasyonun hızla yayılmasının siber saldırıların yürütülmesini kolaylaştırmak için kullanılabileceği de gösterilmiştir (Interpol, 2020). Pandemi süresince bir ayda *oltalama* (phishing) dolandırıcılıklarının yüzde 667 arttığı tespit edildi (ENISA, 2020). Genellikle koronavirüs temalı dezenformasyon,

siber saldırganlar tarafından yaygın olarak kullanılmaktadır. COVID-19'un ilk günlerinde, koronavirüs temalı spam'de yüzde 6.000 fazla artış oldu (Whitmore, &Parham, 2020). COVID-19 sorunlarının bolluğunda birçok gizli tehdit var. Saldırganlar, marka gibi görünmek için COVID-19 dezenformasyonunu kullanmaktadır böylece bir dizi kötü amaçlı spam, kimlik avı saldırısı ve fidye yazılımıyla çalışanları ve müşterileri kandırmaktadır (Deloitte, 2020). Siber tehditler ve riskler, özellikle pandemi esnasında önemli ölçüde artış göstermiş ve ardından yüksek seviyelerde kalmaya devam etmiştir. Ayrıca, sağlık ve finansal hizmetler gibi sektörlerde büyük güvenlik sorunları ile karşı karşıya kalınmıştır (Panda, 2020).

Medya sektöründe de sürekli olarak bir değişim söz konusudur. Teknoloji ve dijital dönüşüm bu değişimin temel sebeplerindendir (Martens ve diğerleri, 2018). 19. yüzyılın sonlarında medya endüstrisinde çok büyük dönüşümler yaşanmıştır. Bu dönüşüm, Sarı Basın adı verilen yeni bir raporlama ve iş modelinin ortaya çıkmasından sonra meydana gelmiştir. Özellikle tabloid gazeteler, mezenformasyon ve dezenformasyon gibi yeni habercilik biçimlerine bireyleri ve medya kurumlarını teşvik edebilmektedir. Dijital dönüşümün önemli bir özelliği medya sektörünü, doğrusal bir iş modelinden ve çevrimdışı haber yayıncılığından çok yönlü bir pazar/platform iş modeline ve çevrimiçi haber yayıncılığına geçirmek zorunda bırakmasıdır (Martens ve diğerleri, 2018). Ebetteki bu değişim ve dönüşüm medya sektörü için de birtakım riskleri beraberinde getirmiştir.

Sosyal medya, medya endüstrisindeki bir diğer önemli dönüştürücü yenlik olarak görülmektedir. Sosyal medyanın internet tabanlı olduğu ve yeni bir iletişim kanalını meydana getirdiğini pek çok kaynak onaylamaktadır (Carr & Hayes, 2015; Kaplan & Haenlein, 2019). Gazeteler, bağımsız satış noktalarından dev haber pazarlama endüstrilerine geçişi tamamladılar; sonuç olarak, bu kitle iletişim endüstrisi, seri üretim ve kitlesel pazarlamayı doğurmuştur (Daly, 2018). Bu kitlesel pazarlama, reklamcıların işini büyük ölçüde kolaylaştırdı ve nihayetinde gazeteler reklam gelirlerine daha fazla bağımlı hale geldi (Daly, 2018; Griffin, 2019).

Sahte haberler ve sosyal medya hakkında geniş bir literatür bulunmaktadır. Siyasi kutuplaşma ve sosyal medya üzerine yapılan bir literatür taraması, çevrimiçi platformlarda yanlış bilgi ve propagandanın yaygınlığı konusunda geniş bir akademik yayım olduğu sonucuna varmaktadır (Tucker ve diğerleri, 2018, s. 15). Sahte haberlerin belirli web siteleri aracılığıyla yayılmasına ek olarak, literatürün gözden geçirilmesi ve sentezi, ana akım haber medyasının sahte haberlerin daha fazla yayılmasında önemli ve etkin bir rol oynadığını göstermektedir (Tsfati ve diğerleri, 2020). Sahte haberlerle ilişkili birçok olgunun nasıl tanımlanacağı konusunda akademik literatürde çok fazla fikir birliği yoktur (Tucker ve diğerleri, 2018).

Dezenformasyon, sosyal medyanın önemli bir özelliğidir. Birçok siyasi aktör, sosyal medya platformlarında dezenformasyonun yayılmasına ve bunu güçlenmek için kullanmaya dahil olmaktadır (Bradshaw & Howard, 2018). Dünya çapında düzenli internet kullanıcılarının yarısından fazlası, sosyal medya platformlarındaki dezenformasyon tehdidinden endişe duymaktadır (Knuutila ve diğerleri, 2020). Sahte haber siteleri, politikacılar, partizan medya, ana akım medya, hükümetler ve diğer aktörler, sosyal medya ekosisteminde dezenformasyon üretme ve yayma konusunda örtüşen rollere sahiptir (Tucker ve diğerleri, 2018). Dezenformasyonun yayılmasına katkı sağlama konusunda motivasyonlar da farklı olabilir. Siyasi motivasyonları olan devlet destekli aktörler dezenformasyon kampanyalarına katılmaktadır. Öte yandan, küçük Veles kasabasından mali teşviklerle Kuzey Makedon gençleri, reklam tıklamaları için ödeme almak için sahte haberleri yaymak amacıyla ABD'de 140'tan fazla siyasi web sitesi açtı (Kshetri & Voas, 2017). Kuzey Makedon aktörlerin durumu, sosyal medyada finansal motivasyon, değer yaratma ve iş modelleri gibi daha geniş bir konuya ışık tutmaktadır. Etki, sosyal medya pazarlamasında anahtar bir kavram olduğundan, sektörler, önemli bir gelir akışı olan reklamlara erişimlerini ve tıklamalarını artırmanın yollarını aramaktadır (Hanna ve diğerleri, 2011).

Diğer taraftan ABD Hazine Bakanlığı'nın Siber Yaptırımlar Programı 2015'te başladı. Ülke dışından siber destekli faaliyetlerin ABD ulusal güvenliğine, dış politikasına ve ekonomisine yönelik olağandışı ve olağanüstü tehdidini ele almak için ulusal acil durum ilan etti ve 2016'da bu ilanda değişiklikler yaptı. Sektörleri, diğer şeylerin yanı sıra, siber etkin ticari veya rekabet avantajı veya özel mali kazanç yoluyla ABD dışından zimmete para geçirmeye ve ticari sır hırsızlığına karşı koruyan bir çerçevedir (ABD Hazine Bakanlığı, 2017). Bakanlık bu çerçeveyi uyguladı ve 2016 seçimlerini ve diğer çeşitli kötü niyetli faaliyetleri bozmak için siber operasyonlara yaptırımlar uyguladı (ABD Hazine Bakanlığı, 2018). Tipik olarak devletler veya devlet destekli aktörler tarafından gerçekleştirilen, fikri mülkiyet ve sektörlere yönelik siber saldırılar karmaşıktır, APT kimlik avı ve dezenformasyon kullanımını içerir. Siber riskler jeopolitik ve ticaret gibi diğer alanlara da yayılmıştır. Siber iddialar, ABD-Çin ticaret anlaşmazlığını sona erdirmeyi amaçlayan ticaret müzakerelerinin bir parçasıydı (Mitchell & Politi, 2019). Bu durum, bu tür bir siber tehdidin sektörler için önemli bir risk olmaya devam edebileceğini göstermektedir.

4. BİLGİ BOZUKLUĞU İLE SAVAŞ VE SEKTÖREL RİSKLERİ YÖNETME

Mezenformasyon ve dezenformasyon, kamu sektörü ve özel sektör için önemli siber riskler oluşturmaktadır. Dijital çağda dördüncü sanayi devriminin etkilerine tanık olurken, başta sağlık, medya ve finans sektörleri olmak üzere tüm sektörlerde dijital dönüşüm trendinin hâkim olduğu gözlemlenmektedir. Dijital dönüşümle yüzleşmek için sektörler öncelikle hangi teknolojilerin alakalı olduğunu ve iş ortamlarında nasıl uygulanacağını belirlemelidir (Saarikko et al., 2020). Sunucu ve yedekleme alanı olarak kullanılan donanım ve yazılımlardan oluşan eski sistemlerin güvenlik açıkları oluşturduğu ve riski artırdığı yaygın olarak kabul edilmektedir.

İlk olarak, sektör liderleri ve yöneticilerin siber riskin varlığını tanıması gerekir. Siber tehditleri tespit etmek için onları tespit etme yeteneğine sahip olmak çok önemlidir. Sağlık kuruluşlarının siber tehditleri etkili bir şekilde anlama, izleme, raporlama ve yönetme konusundaki sınırlı bir etkinlik alanı bulunmaktadır (Bell ve Ebert, 2015). Pandemi sırasında siber saldırılar daha karmaşık hale geldikçe ve hacimleri önemli ölçüde arttığından bu sorun daha da kötüleşmektedir. Bu tespit sadece sağlıkta değil, diğer alanlarda da bir sorundur. Saldırganlar yöntemlerini geliştirir ve uyarlar; örneğin, kimlik avcıları, tespit edilmekten kaçınmak için güvenliği ihlal edilmiş bir etki alanında bulunabilirler (Jang-Jaccard & Nepal, 2014). Birçok kuruluş bunu fark etmeyebilir ve 2019'daki gibi tüm ihlallerin dörtte birinin aylarca fark edilmemesi gibi olumsuz sonuçlar ortaya çıkabilir (Champion, 2020). Bir diğer önemli eylem, yanıltıcı bilgilerden kaynaklanan siber riskleri ve bunların iş üzerindeki etkilerini anlamaktır. Dezenformasyon ve mezenformasyon gibi bu risklerden bazıları nispeten kolay bir şekilde tanınabilir ve anlaşılabilirken, bazı sorunları değerlendirmek daha zordur. Bu anlamda, bilgi bozukluğunun etkisini yakalayan uygun bir risk değerlendirme çerçevesi esastır.

Dezenformasyon Davranış Kuralları, sektörlerin gönüllü olarak imza attığı küresel bir öz-düzenleyici standartlar organıdır (Avrupa Komisyonu, 2018). Etkili bir standardın iki temel unsuru olmalıdır: Ampirik olarak türetilen teknik veriler ile niteliksel yargılar ve risk toleransı ve strateji gibi yönetsel perspektifler arasındaki boşluğu kapatmak için hem risk değerlendirmesi hem de karar verme modellerini içermelidir (Collier ve diğerleri, 2014).

Dezenformasyonla mücadele için bir dizi araç bulunmaktadır. Bu araçlar, insan doğrulayıcıları olan web sitelerinden botları tespit etmek için yapay zekâ kullanan uygulamalara kadar pek çok biçimde gelir ve birkaç kategoriye ayrılır (RAND, 2019):

(1) bot/spam algılama,

(2) kodlar ve standartlar,

(3) güvenilirlik değerlendirmesi,

(4) dezenformasyon takibi,

(5) eğitim ve öğretim,

(6) doğrulama,

(7) beyaz listeye alma.

Kuruluşlar, dijital dönüşümlerine, genel stratejilerine ve yanıltıcı bilgilerden siber riski yönetme yöntemlerine en uygun olanı seçmelidirler.

Ortaklıkların birçok faydası olabilir. Birincisi, standartların ve ulusal, sektörel veya sektöre özel kılavuzların geliştirilmesini kolaylaştırabilirler. İkincisi, ortaklıklar siber savunmada ölçek ve ölçek ekonomileri yaratır. Üçüncüsü ve en önemlisi, birçok durumda, yüksek düzeyde yaratıcı ve karmaşık devlet destekli saldırıların oluşturduğu siber riskleri azaltmak, kuruluşlar için imkânsız veya son derece maliyetlidir. Bu nedenle, bu siber risklerin ele alınmasında kamu sektörü ile iş birliği, muhtemelen kamu-özel sektör ortaklıkları şeklinde çok önemlidir.

Yukarıdaki önerileri uygulamak için sektörler yeterli fon yatırımı yapmalıdır. Mevcut dezenformasyonla mücadele araçları ve yöntemleri olmasına rağmen, dördüncü sanayi devriminin ilerlemesiyle birlikte yeni teknolojiler gelişmektedir. Bu nedenle araştırma ve geliştirme için daha fazla harcama yapmak kurumlar için önemli hale gelmektedir. Bilgi bozukluğuna ilişkin tedbiren yazılımların edinilmesi, siber savunma harcamaları yapmak da önemli bir konu olarak değerlendirilmelidir. Aynı zamanda her kurumun bir dijital dönüşüm stratejisi olmalı ve bu stratejik planda, siber riskler ve riskler sonrası kayıpları azaltmaya yönelik kriz yönetimi programları gibi işler için gerekli finansal kaynağın ayrılması önemlidir

SONUÇ

Yeni iletişim teknolojilerinin gelişimine paralel olarak gerçekleşen hızlı değişim gündelik hayatı da büyük ölçüde etkilemiştir. Eğitimden, pazarlamaya, iş hayatına, sağlık alanına kadar birçok alanda yeni iletişim teknolojilerinin kullanılmasıyla dezenformasyon ve mezenformasyon artış göstermiştir. Dezenformasyon ve mezenformasyonun artışı bireyler ve toplumlar açısından ciddi tehditler oluştururken kamu sektörü ve özel sektör açısından da gelişmiş kalıcı tehditler oluşturabilmektedir. Bu durum dijital toplum içerisinde varlık sürdürmeye çalışan sektörler açısından oldukça önemli bir sorun olarak karşımıza çıkmaktadır. Bu nedenle bu tehditlere karşı tedbirlerin alınması güvenli teknolojilerin kullanılması bir zorunluluk haline gelmiştir. Aksi halde bilgi bozukluğu olumsuz birçok problem yaratarak iş akışını bozabilmektedir. Özellikle dünyada yaşanan COVID-19 ile birlikte kitle iletişim araçlarından dijital teknolojilerin zorunlu bir şekilde kullanımı bilgi bozukluğunun artmasına neden olmuştur.

Özel sektör, kamu kurum/kuruluşları ve toplumların dijital dönüşümü yeni riskler getirmekte ve sektörler için ortaya çıkan yeni bir tehdit bulunmaktadır. Ortaya çıkan bu tehdit bilgi bozukluğudur. Bilgi bozukluğu genellikle mezenformasyon ve dezenformasyon şeklinde meydana gelmektedir. Bu çalışma, bilgi bozukluğunun, türü fark etmeksizin, sektörel etkisini ve sektörlerin iletişim teknolojilerini kullanması ile birlikte karşılaşacağı muhtemel riskleri anlamaya çalışmıştır. Bu riskler sektörü pek çok açıdan tehdit edebilmektedir. Dolayısıyla konunun daha iyi anlaşılması ve ortaya konması için ileri çalışmalara ve başkaca akademik araştırmalara ihtiyaç olduğu düşünülmektedir. Son olarak, bu çalışma siber riskte bilgi bozukluğu ile başa çıkmak için bazı öneriler sunmaktadır: Dijital dönüşüm stratejileri oluşturmak, siber riskleri belirlemek ve değerlendirmek, standartlar ve normlar belirlemek ve benimsemek, mezenformasyon ve dezenformasyonu önleme ve çeşitli endüstriler, sektörler ve uluslararası liderlerle ve liderlere fayda sağlayabilecek ortaklıklarla yatırımları artırmak.

KAYNAKÇA

ABD Hazine Bakanlığı (2017). Cyber-related sanctions program. Washington, DC: DoT.

ABD Hazine Bakanlığı. (2018). Treasury sanctions Russian cyber actors for interference with the 2016 U.S. elections and malicious cyber-attacks. Available at https:// home.treasury.gov/news/press-releases/sm0312

APWG. (2020, August 27). Phishing activity trends report, 2nd quarter 2020. Anti-Phishing Working Group. Available at https://docs.apwg.org/reports/apwg_trends_report_q2_ 2020.pdf

Avrupa Komisyonu (2018). Final report of the high-level expert group on fake news and online disinformation. Available at https://ec.europa.eu/digital-single-market/ en/news/final-report-high-level-expert-group-fake-newsand-online-disinformation

Avrupa Sayıştayı (2020). EU action plan against disinformation. Available at https://www.eca.europa.eu/ Lists/ECADocuments/AP20_04/AP_Disinformation_EN.pdf

Bell, G., & Ebert, M. (2015). Health care and cyber security: Increasing threats require increased capabilities. KPMG. Available at https://assets.kpmg/content/dam/kpmg/pdf/ 2015/09/cyber-health-care-survey-kpmg-2015.pdf

Boddy, M. (2018). Phishing 2.0: The new evolution in cybercrime. Computer Fraud & Security, 2018(11), 8e10.

Bradshaw, S., & Howard, P. (2018). The global organization of social media disinformation campaigns. Journal of International Affairs, 71(1.5), 23e32.

Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. Atlantic Journal of Communication, 23(1), 46e65.

Champion, A. (2020, October). Cyber-attack detection challenges and how to meet them. F-secure. Available at https://www.f-secure.com/gb-en/consulting/our-thinking/ challenges-of-cyber-attack-detection

CIS. (2021). Cybersecurity spotlight: Cyber threat actors. Center for Internet Security. Available at https://www. cisecurity.org/spotlight/cybersecurity-spotlight-cyberthreat-actors/

Cisco. (2020). What are the most common cyber-attacks?. Available at https://www.cisco.com/c/en/us/products/ security/common-cyberattacks.html

Collier, Z. A., Dimase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014). Cybersecurity standards: Managing risk and creating resilience. Computer, 47(9), 70e76.

Daly, C. B. (2018). Covering America: A narrative history of a nation's journalism. Amherst, MA: University of Massachusetts Press.

Deloitte. (2020). COVID-19 executive cyber briefing. Available at https://www2.deloitte.com/global/en/pages/risk/covid-19/global-cyber-covid-19-weekly-executive-cyber-briefing.html

ENISA. (2020). ENISA threat landscape. European Union Agency for Cybersecurity. Available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Griffin, B. (2019). Yellow journalism, sensationalism, and circulation wars. New York, NY: Cavendish Square Publishing.

Hanna, R., Rohm, A., & Crittenden, V. L. (2011). We're all connected: The power of the social media ecosystem. Business Horizons, 54(3), 265e273.

ICC. (2020). COVID-19 cyber security threats to MSMEs. International Chamber of Commerce. Available at https://iccwbo.org/content/uploads/sites/3/2020/05/2020-icc-soscybersecurity.pdf

Interpol. (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Lyon, France: International Criminal Police Organization.

Ireton, C., & Posetti, J. (2018). Journalism, 'fake news,' and disinformation. Paris, France: UNESCO.

ISACA. (2020). State of cybersecurity 2020. Schaumburg, IL: Information Systems Audit and Control Association.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973e993. J

Kaplan, A., & Haenlein, M. (2019). Digital transformation and disruption: On big data, blockchain, artificial intelligence, and other things. Business Horizons, 62(6), 679e681.

Knuutila, A., Neuder, L., & Howard, P. (2020). Global fears of disinformation. Oxford, UK: Oxford University Press.

Kshetri, N., & Voas, J. (2017). The economics of "fake news." IT Professional, 19(6), 8e12.

Martens, B., Aguiar, L., Gomez-Herrera, E., & Mueller-Langer, F. (2018). The digital transformation of news media and the rise of disinformation and fake news. Digital Economy Working Paper 2018-02, Joint Research Centre Technical Reports. Available at https://dx.doi.org/10.2139/ssrn. 3164170

Mitchell, T., & Politi, J. (2019, April 30). Trump drops cyber theft demands in bid for swift trade deal with China. Financial Times. Available at https://www.ft.com/content/ 3cb5bfda-6b0e-11e9-80c7-60ee53e6681d

NATO. (2020). Media e (Dis)information e security. Available at https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal1-fake-news.pdf

Nemr, C., & Gangware, W. (2019). Weapons of mass distraction: Foreign state-sponsored disinformation in the digital age. Park Advisors. Available at https://www.state.gov/wpcontent/uploads/2019/05/Weapons-of-Mass-DistractionForeign-State-Sponsored-Disinformation-in-the-Digital-Age. pdf

NIST. (2015). Security and privacy controls for federal information systems and organizations. Washington, DC: National Institute for Standards and Technology. OSCE. (2017). Joint declaration on freedom of expression and "fake news," disinformation and propaganda. Vienna, Austria: Organization for Security and Co-Operation in Europe.

Oxford İngilizce Sözlüğü. (2020). Oxford, UK: Oxford University Press.

Panda. (2020). 43 COVID-19 cybersecurity statistics. Available at https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/ Parham, G., &

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage: The information revolution is transforming the nature of competition. Harvard Business Review, 63(4), 149e160.

RAND. (2019, December 19). Fighting disinformation online: A database of web tools. Available at https://www.rand.org/ research/projects/truth-decay/fighting-disinformation. html

Saarikko, T., Westergren, U. H., & Blomquist, T. (2020). Digital transformation: Five recommendations for the digitally conscious firm. Business Horizons, 63(6), 825e839.

Schwab, K. (2017). *The fourth industrial revolution*. Currency.

Tsfati, Y., Boomgaarden, H. G., Stro¨mba¨ck, J., Vliegenthart, R., Damstra, A., & Lindgren, E. (2020). Causes and consequences of mainstream media dissemination of fake news: Literature review and synthesis. Annals of the International Communication Association, 44(2), 157e173.

Tucker, J., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., et al. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. Hewlett Foundation. Available at https://www. hewlett.org/wp-content/uploads/2018/03/Social-MediaPolitical-Polarization-and-Political-DisinformationLiterature-Review.pdf

Whitmore, G. P. W., & Parham, G. (2020). „COVID-19 cyberwar: How to protect your business,". *IBM Institute for Business Value, Iunie*.