Üçüncü Sektör Sosyal Ekonomi Dergisi
Third Sector Social Economic Review
61(2) 2026, 2343-2367
doi: 10.63556/tisej.2026.1856

Araştırma Makalesi

Proaktif Kişilik ve Bireysel Siber Güvenliğin Tekno-Stres Üzerindeki Etkisi: Havacılık Sektörü Çalışanlarına Yönelik Bir Araştırma

The Impact of Proactive Personality and Individual Cybersecurity on Technostress: A Study on Aviation Sector Employees

Ahmet DENİZ
Dr. Öğr. Üyesi, İstanbul Gelişim Üniversitesi
Uygulamalı Bilimler Fakültesi
ahdeniz@gelisim.edu.tr
https://orcid.org/0000-0002-3878-6331

Makale Geliş Tarihi	Makale Kabul Tarihi
03.03.2026	31.05.2026

Öz

Bu araştırma, havacılık sektörü çalışanlarının proaktif kişilik özellikleri ile bireysel siber güvenlik davranışlarının tekno-stres düzeyleri ile ilişkisini ve yordayıcı rollerini incelemeyi amaçlamaktadır. Dijitalleşmenin hızla yaygınlaştığı günümüz iş ortamlarında, çalışanların teknolojiye bağlı stres faktörlerine verdikleri tepkiler giderek daha fazla önem kazanmaktadır. Bu bağlamda çalışmada, bireysel düzeydeki kişilik özellikleri ile siber güvenlik davranışlarının tekno-stres ile anlamlı biçimde ilişkili olup olmadığı ele alınmıştır. Araştırma nicel yöntemle yürütülmüş olup, Türkiye'de havacılık sektöründe görev yapan 387 çalışandan anket tekniğiyle veri toplanmıştır. Elde edilen veriler; korelasyon analizi, bağımsız örneklem t-testi, grup karşılaştırma testleri ve çoklu doğrusal regresyon analizi kullanılarak değerlendirilmiştir. Bulgular, proaktif kişiliğin tekno-stres ile negatif yönlü, bireysel siber güvenlik davranışlarının ise pozitif yönlü ve anlamlı ilişkiler sergilediğini ve her iki değişkenin tekno-stresin anlamlı yordayıcıları olduğunu göstermektedir. Ayrıca demografik değişkenlere göre yapılan karşılaştırmalarda cinsiyet, medeni durum, statü, yaş, eğitim düzeyi ve kıdem açısından bazı araştırma değişkenlerinde anlamlı farklılıklar tespit edilmiştir. Araştırma sonuçları, çalışan refahını artırmak isteyen örgütlerin proaktif kişilik özelliklerini destekleyen uygulamalar geliştirmelerinin ve siber güvenlik eğitimlerini stres yönetimiyle birlikte ele almalarının yararlı olabileceğine işaret etmektedir.

Anahtar Kelimeler: *Proaktif Kişilik, Tekno-Stres, Bireysel Siber Güvenlik, Havacılık Sektörü, Örgütsel Davranış*

Abstract

This study aims to examine the relationships between proactive personality traits and individual cybersecurity behaviors and technostress levels, as well as their predictive roles, among employees in the aviation sector. In today's rapidly digitalizing work environments, employees' responses to technology-related stressors have become increasingly important. Within this context, the study investigates whether individual-level personality traits and cybersecurity behaviors are significantly associated with technostress. The research was conducted using a quantitative method, and data were collected through a questionnaire from 387 employees working in the aviation sector in Türkiye. The data were analyzed using correlation analysis, independent samples t-test, group comparison tests, and multiple linear regression analysis. The findings indicate that proactive personality is negatively associated with technostress, whereas individual cybersecurity behaviors are positively associated with

Önerilen Atıf /Suggested Citation

Deniz, A., 2026, Proaktif Kişilik ve Bireysel Siber Güvenliğin Tekno-Stres Üzerindeki Etkisi: Havacılık Sektörü Çalışanlarına Yönelik Bir Araştırma, *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 61(2), 2343-2367.

technostress; both variables are significant predictors of technostress. In addition, comparisons based on demographic variables revealed significant differences in some research variables according to gender, marital status, occupational status, age, education level, and tenure. The results suggest that organizations seeking to enhance employee well-being may benefit from developing practices that support proactive personality traits and integrating cybersecurity training with stress management.

Keywords: *Proactive Personality, Technostress, Individual Cybersecurity, Aviation Sector, Organizational Behavior*

1. GİRİŞ

Günümüzde iş yaşamının dijitalleşmesiyle birlikte teknoloji, örgütlerin temel yapı taşı hâline gelmiş; iş süreçleri, karar alma mekanizmaları ve iletişim biçimleri dijital platformlara entegre olmuştur. Bu dönüşüm, özellikle yüksek teknolojiye bağımlı sektörlerde çalışan bireylerin teknolojiyle olan etkileşimini yoğunlaştırarak, geleneksel stres kavramına yeni bir boyut eklemiştir. Bu bağlamda ortaya çıkan tekno-stres, bireylerin bilgi ve iletişim teknolojilerine maruz kaldıklarında hissettikleri psikolojik ve fiziksel zorlanmaları ifade etmektedir (Tarafdar, Tu, Ragu-Nathan ve Ragu-Nathan, 2007).

Dijitalleşmenin hızla arttığı ve bilgi teknolojilerinin yoğun şekilde kullanıldığı iş ortamlarında, çalışanların teknolojiye karşı verdikleri psikolojik tepkiler önemli bir araştırma konusu hâline gelmiştir. Havacılık sektörü, iş güvenliği, zaman baskısı, yoğun veri kullanımı ve sürekli teknoloji takibi gibi unsurlar nedeniyle tekno-stresin yüksek düzeyde hissedilebildiği sektörlerin başında gelmektedir. Uçuş güvenliğinden yer destek operasyonlarına kadar pek çok süreç, dijital sistemlerle bütünleşmiş hâlde yürütülmektedir. Bu nedenle, bu sektörde çalışan bireylerin teknoloji kaynaklı stresle baş etme biçimleri, yalnızca bireysel refah değil, aynı zamanda toplumsal güvenlik açısından da önem taşımaktadır.

Literatürde, tekno-stresi etkileyen faktörler arasında örgütsel destek, teknoloji karmaşıklığı ve iş yükü gibi değişkenler geniş biçimde incelenmişken (Tarafdar vd., 2007; Tarafdar, Tu ve Ragu-Nathan, 2011), bireysel kişilik özelliklerinin ve siber güvenlik davranışlarının tekno-stres üzerindeki etkisi görece sınırlı kalmıştır. Özellikle bireyin proaktif kişilik düzeyi, çevresel değişkenlere karşı geliştirdiği uyum stratejilerini ve stresle başa çıkma biçimlerini şekillendirmektedir (Bateman ve Crant, 1993). Proaktif bireyler, değişimi önceden öngörebilen, çözüm üretebilen ve riskleri fırsata çevirebilen bireylerdir (Çelik ve Kara, 2017). Bu yönüyle, dijitalleşme kaynaklı stres durumlarıyla daha etkin biçimde baş edebilecekleri varsayılmaktadır. Havacılık sektöründe yapılan güncel çalışmalar, proaktif kişilik özelliğinin çalışanların iş ortamına uyum süreçlerinde ve örgütsel çıktılar üzerinde önemli bir rol oynadığını göstermektedir (Gence, Ural ve Aksu, 2024).

Öte yandan, teknolojik ortamda çalışan bireylerin bireysel siber güvenlik davranışları da önemli bir belirleyici değişken hâline gelmiştir. Dijital cihazların yaygın kullanımı, kişisel veri güvenliğinin korunmasını bireysel bir sorumluluk hâline getirmektedir (Erol, Şahin, Yılmaz ve Haseski, 2015). Bireyin teknolojiyi güvenli ve bilinçli kullanması, yalnızca kurumsal güvenlik algısını değil, aynı zamanda psikolojik güven algısını şekillendirebilmekte ve bu durum bireylerin teknolojiye yönelik stres deneyimleriyle ilişkili olabilmektedir. Dijitalleşmenin artmasıyla birlikte teknolojik taleplerin yoğunlaştığı çalışma ortamlarında, bireylerin karşılaştıkları dijital riskler, artan bilgi yükü ve sürekli erişilebilir olma beklentisinin, çalışanların algıladıkları stres düzeyleriyle pozitif yönde ilişkili olabileceği belirtilmektedir (Altıntaş ve Altıntaş, 2026; Altıntaş, Şanlı ve Odacı, 2026).

Araştırma, bireylerin dijital ortamlarda karşılaştıkları talepleri nasıl algıladıklarını açıklayan Lazarus'un Bilişsel Değerlendirme Kuramı (Lazarus ve Folkman, 1984) çerçevesinde ele alınmıştır. Bu kurama göre bireyler, çevresel uyarıcıları tehdit ya da fırsat olarak değerlendirmekte ve bu bilişsel değerlendirme süreci stres tepkilerini şekillendirmektedir. Bu bağlamda, proaktif kişilik ve siber güvenlik düzeyi, teknolojik risklerin nasıl algılandığını ve bu algının tekno-stres düzeyine nasıl yansıdığını açıklamada önemli değişkenler olarak değerlendirilmektedir.

Bu çalışma, havacılık sektörü çalışanlarının proaktif kişilik özellikleri ile bireysel siber güvenlik davranışlarının tekno-stres düzeyleri ile ilişkisini ve yordayıcı rollerini incelemeyi amaçlamaktadır. Bu kapsamda araştırma, "Proaktif kişilik ve bireysel siber güvenlik davranışları, havacılık sektörü çalışanlarının tekno-stres düzeyleri ile anlamlı biçimde ilişkili midir ve bu değişkenler tekno-stresi ne ölçüde yordamaktadır?" sorusuna yanıt aramaktadır. Literatürde bu üç değişkenin birlikte ele alındığı çalışmaların sınırlı olması, araştırmanın özgün değerini artırmaktadır.

Ayrıca çalışmanın Türkiye bağlamında ve havacılık sektörü gibi yüksek riskli bir alanda gerçekleştirilmesi, araştırmaya hem teorik hem de uygulamaya dönük katkı sunması beklenmektedir. Araştırma bulgularının, örgütsel davranış literatürüne yeni ampirik veriler sunmasının yanı sıra, yöneticiler ve insan kaynakları uygulayıcıları için dijitalleşme sürecinde çalışan refahını artırmaya yönelik politika geliştirme açısından yol gösterici olması beklenmektedir.

2. KURAMSAL TEMELLER

2.1. Proaktif Kişilik

Kavramsal olarak proaktiflik, bireyin yaşamındaki olayların sorumluluğunu üstlenmesi ve karşılaştığı durumları pasif biçimde kabullenmek yerine aktif biçimde şekillendirmesi olarak tanımlanmaktadır (Frankl, 1994). Bu bağlamda proaktiflik, bireyin kendi yaşamını yönlendirme ve değiştirme cesareti olarak değerlendirilmektedir. Bateman ve Crant (1993), proaktif bireyleri fırsatları önceden görebilen, inisiyatif alabilen ve çevresel koşulları dönüştürme eğilimi gösteren kişiler olarak tanımlamıştır.

Proaktif kişilik, her bireyde aynı düzeyde bulunmayan ve kişinin çevresinde gerekli gördüğü değişimleri başlatma isteğini ifade eden bir kişilik özelliğidir (Bolino, Valcea ve Harvey, 2010). Bu bireyler sorumluluk alma, risk üstlenme ve kararlı davranma eğilimleriyle öne çıkmakta; hedeflerine ulaşmak için sistemli biçimde çaba göstermektedirler (Crant, 1995). Yanı sıra proaktif kişilik özellikleri taşıyan bireyler karar verme aşamasında kendi değerleri doğrultusunda ilerlerler (Covey, 2010). Ayrıca proaktif bireyler, aldıkları kararların sonuçlarının sorumluluğunu üstlenme eğiliminde olup, yaşamlarını dış koşullardan ziyade kendi tercihleri doğrultusunda yönlendirmektedirler (Crant ve Bateman, 2000).

Literatürde proaktif kişilik özelliklerine sahip bireylerin değişime uyum sağlama becerilerinin yüksek olduğu vurgulanmaktadır (Caprara ve Cervone, 2003). Bu bireyler, çevresel belirsizlikler karşısında başarısızlık yerine uyum sağlamayı tercih etmekte ve karşılaştıkları sorunlara çözüm odaklı yaklaşmaktadırlar. Yanı sıra proaktif kişilik özelliklerini güçlü biçimde taşıyan bireylerin sorumluluk alma konusunda gönüllü olan kararlı kişiler oldukları söylenebilir (Antonacopoulou, 2000). Bu özellikleri sayesinde hızlı teknolojik dönüşümlerin yaşandığı çalışma ortamlarında daha etkin performans gösterebilmektedirler (Fuller ve Marler, 2009).

Proaktif bireylerin önemli özelliklerinden biri de güçlü içsel motivasyona sahip olmalarıdır. Ortaya çıkan fırsatları başarılı şekilde öngörebildiklerinden gerekli olan ihtiyaçları da önceden belirleyerek işlevsel planlamalar yapabilirler, stratejik kararlar alabilirler (Lee ve Peterson, 2000). Bu bireyler, hedeflerine ulaşma sürecinde dışsal yönlendirmeye ihtiyaç duymadan sorumluluk alabilmekte ve stresle daha etkili başa çıkma eğilimi gösterebilmektedirler (Bateman ve Crant, 1999). Ayrıca yeni bilgiler öğrenmeye açık olmaları, öngörü yeteneklerinin gelişmiş olması ve iletişim becerilerinin güçlü olması, proaktif bireylerin iş yaşamında daha etkili olmalarını sağlamaktadır (Gupta ve Bhawe, 2007; Thompson, 2005).

Proaktif kişilik ile stres arasındaki ilişkiyi inceleyen çalışmalarda, proaktif başa çıkma davranışları sergileyen bireylerin daha düşük stres düzeyine sahip oldukları belirlenmiştir (Verešová ve Malá, 2012). Benzer şekilde, Uncuoğlu ve Çakmak (2017), proaktif kişilik ile proaktif çalışma davranışı arasındaki ilişkide psikolojik güçlendirmenin düzenleyici rolünü ortaya koymuştur. Seibert, Kraimer ve Crant (2001) ise proaktif bireylerin çevresel stres kaynaklarına karşı daha dirençli olduklarını vurgulamaktadır.

Proaktif kişilik düzeyinin ölçümünde Claes, Beheydt ve Lemmens (2005) tarafından geliştirilen ve Akın, Abacı, Kaya ve Arıcı (2011) tarafından Türkçeye uyarlanan Proaktif Kişilik Ölçeği kısa formu yaygın olarak kullanılmaktadır. Bu ölçek, bireyin inisiyatif alma, değişim yaratma ve sonuç odaklı davranma eğilimlerini değerlendirmektedir. Yeşil (2022) çalışmasında, proaktif kişiliğin mesleki doyum, örgütsel bağlılık ve psikolojik sağlamlık ile pozitif ilişkili olduğunu ortaya koymuştur. Proaktif kişilik özelliğinin çalışan davranışları üzerinde belirleyici bir rol oynadığı ve örgütsel süreçlerde aktif katılımı artırdığı da çeşitli araştırmalarla ortaya konulmuştur (Çoban ve Bükeç, 2021).

Ayrıca literatürde, proaktif bireylerin teknolojiye uyum sürecinde daha başarılı olduğu ve teknolojik yenilikleri bir tehditten ziyade fırsat olarak değerlendirdiği belirtilmektedir (Fuller ve Marler, 2009). Bu bireyler yeni sistemlere entegrasyonda daha hızlı hareket eder, iş süreçlerini yeniden yapılandırmada istekli davranırlar ve bu durum onların tekno-stres yaşama olasılıklarını azaltabilir. Genel olarak

değerlendirildiğinde, proaktif kişilik özelliklerine sahip bireylerin değişime açık olmaları, problem çözme becerilerinin gelişmiş olması ve içsel motivasyonlarının yüksekliği sayesinde teknoloji yoğun çalışma ortamlarında karşılaştıkları stres faktörleriyle daha etkili biçimde başa çıkabildikleri söylenebilir.

Bu çerçevede, proaktif kişilik düzeyinin çalışanların tekno-stres algıları ile negatif yönde ilişkili olabileceği değerlendirilmektedir. Dolayısıyla proaktif kişilik düzeyinin tekno-stres ile ilişkisi ve tekno-stresi yordama düzeyinin ampirik olarak incelenmesi önem arz etmektedir.

2.2. Tekno-Stres

Tekno-stres, bireylerin bilgi ve iletişim teknolojilerini kullanırken yaşadıkları stres durumlarını tanımlayan bir kavramdır. Kavramsal temeli Brod (1984) tarafından atılan bu olgu, dijitalleşmenin bireysel psikoloji üzerindeki etkilerini açıklamaya yöneliktir. Tekno-stres, bireyin bilgi ve iletişim teknolojilerine maruz kalması sonucu yaşadığı psikolojik baskı durumudur (Cadieux, Cadieux, Youssef ve Mosconi, 2020). Dijital çağda bireyler ve kurumlar hızla değişen teknolojilere uyum sağlamak zorunda kalmakta; ancak bu süreç her birey için sorunsuz ilerlememektedir. Teknolojik araçların yoğun ve karmaşık kullanımı, bireylerde psikolojik stres belirtilerine yol açmakta ve bu durum literatürde tekno-stres kavramı ile açıklanmaktadır (Norhisham, 2021).

Tarafdar vd. (2007), tekno-stresi beş alt boyut altında incelemiştir: tekno-aşırı yük, tekno-istila, tekno-belirsizlik, tekno-karmaşıklık ve tekno-güvensizlik. Bu boyutlar, bireylerin farklı düzeylerde teknoloji kaynaklı stres yaşamasına neden olmakta ve psikolojik dayanıklılıklarını sınamaktadır. Tekno-stres, yeni bilgisayar teknolojileriyle sağlıklı biçimde başa çıkamamanın neden olduğu modern bir uyum problemi olarak da tanımlanmaktadır.

Tarafdar vd. (2007)'in çalışmasına dayanan ve Ilgaz, Özgür ve Çuhadar (2016) tarafından Türkçeye uyarlanan Tekno-Stres Ölçeği, bireylerin dijital iş ortamlarında yaşadığı stresin çok boyutlu biçimde değerlendirilmesine olanak sağlamaktadır. Literatürde, tekno-stresin çalışanlarda tükenmişlik, düşük iş performansı, örgütsel bağlılıkta azalma ve işten ayrılma niyeti gibi olumsuz sonuçlara yol açtığına dair güçlü bulgular bulunmaktadır (Ayyagari, Grover ve Purvis, 2011; Ragu-Nathan vd., 2008). Dijitalleşmenin yoğun olduğu çalışma ortamlarında artan teknolojik taleplerin çalışanların bilişsel ve duygusal yükünü artırarak tekno-stres düzeyleriyle ilişkili olabileceği belirtilmektedir (Altıntaş ve Altıntaş, 2026).

Tekno-stres, dijitalleşen dünyada bireylerin ruhsal, zihinsel ve fiziksel sağlığını etkileyen önemli bir araştırma alanı olarak değerlendirilmektedir. Eğitimden sağlığa, akademiden özel sektöre kadar çok çeşitli alanlarda karşımıza çıkan bu olgu hem bireysel hem de kurumsal düzeyde ele alınması gereken çok boyutlu bir problemdir. Teknolojinin faydalarından maksimum düzeyde yararlanmak için, tekno-stresin farkında olunmalı ve etkilerini azaltacak politika ve uygulamalar hayata geçirilmelidir. Tekno-stresin olumsuz etkilerini azaltmaya yönelik olarak çalışanların dijital yeterliliklerinin artırılması, teknoloji kullanımına yönelik eğitim programlarının geliştirilmesi ve kurumsal destek mekanizmalarının güçlendirilmesi önerilmektedir. Ayrıca kullanıcı dostu sistemlerin tercih edilmesi, esnek çalışma düzenlemeleri ve psikolojik destek hizmetlerinin sunulması, teknoloji kaynaklı stresin azaltılmasına katkı sağlamaktadır (Salanova, Llorens ve Cifre, 2013).

Tekno-stres düzeyini belirleyen temel unsurlar arasında bireyin teknolojiyle başa çıkma becerisi, teknolojik yeterlilik düzeyi, destek sistemlerinin varlığı ve kişilik özellikleri yer almaktadır (Tarafdar, Tu ve Ragu-Nathan, 2011). Havacılık sektöründe artan dijitalleşme ile birlikte teknolojik sistemlerin karmaşıklığı, sürekli güncellenme gereksinimi ve artan bilgi akışı gibi faktörlerin çalışanlar üzerinde stres oluşturabildiği ifade edilmektedir (Altıntaş, Şanlı ve Odacı, 2026).

Havacılık sektörü çalışanları, yoğun dijital sistem kullanımı nedeniyle tekno-stres riski yüksek gruplar arasında yer almaktadır. Bu nedenle, bu çalışanların teknoloji kaynaklı stresle başa çıkma süreçlerinde bireysel siber güvenlik davranışları ve proaktif kişilik özellikleri önemli değişkenler arasında değerlendirilmektedir. Dolayısıyla bu çalışmada, söz konusu bireysel faktörlerin tekno-stres ile ilişkisi ve tekno-stresi yordama düzeylerinin incelenmesi, literatürdeki önemli bir boşluğu doldurmayı amaçlamaktadır.

2.3. Bireysel Siber Güvenlik

Siber Güvenlik; teknolojik gelişmelerin bir sonucu olarak yakın tarihte önemli bir gündem konusu olarak literatürdeki yerini almıştır. Özellikle internet kullanıcılarının sayısının artması ve kullanıcı profillerinin çeşitlenmesi çeşitli güvenlik sorunlarının ortaya çıkmasına neden olmuştur. Bu sorunlar aynı zamanda maddi zararlara ve psikolojik veya fiziksel zararlara yol açmıştır. Virüsler, spamlar, bilgisayar korsanlığı faaliyetleri, kimlik avı, reklam dolandırıcılığı, siber zorbalık, istismar, terör ve gizlilik ihlalleri internette sıkça karşılaşılan konulardır (Kim, Jeong, Kim ve So, 2011).

Tüm bu tehditler bazen maddi hasara yol açabilmekte ve hatta zaman zaman hayati tehlike yaratabilmektedir. Ancak temel önlemlerle sanal dünyanın bazı gerçek tehlikelerinden kaçınmak mümkündür. Bu önlemler bireysel olabileceği gibi mevzuat yoluyla da alınabilir. Literatür, her yaştan, meslekten ve sosyal çevreden internet ve bilgisayar kullanıcısının siber güvenlik riskleri konusunda farkındalığının düşük olduğunu göstermektedir (Çubukçu ve Bayram, 2013).

İnternet kullanımının yaygınlaşmasıyla ortaya çıkan riskler, bireyleri yalnızca psikolojik ve fiziksel açıdan değil; aynı zamanda sosyal ve ekonomik boyutlarda da olumsuz etkileyebilmektedir (Çubukçu ve Bayram, 2013). Virüsler, istenmeyen e-postalar (spam), bilgisayar korsanlığı (hacking), oltalama (phishing) ve reklam dolandırıcılığı gibi tehditler doğrudan teknoloji temelli riskler arasında yer almaktadır. Bunun yanında siber zorbalık, istismar, terör faaliyetleri ve gizlilik ihlalleri gibi unsurlar ise teknoloji aracılığıyla ortaya çıkmakla birlikte daha geniş sosyal boyutlara sahip riskler olarak değerlendirilmektedir.

De Moor vd. (2008), çevrimiçi tehditleri farklı kategoriler altında sınıflandırmıştır. Buna göre nefret söylemi, şiddet, ırkçılık, yanlış bilgilendirme, olumsuz propaganda ve pornografik içerikler "içerik" kapsamında ele alınırken; siber zorbalık, cinsel istismar ve gizlilik ihlalleri "temas" başlığı altında değerlendirilmektedir. Oltalama saldırıları, zararlı (casus) yazılımlar, kimlik hırsızlığı ve dolandırıcılık faaliyetleri ise "ticari riskler" kategorisinde incelenmektedir (Valcke, Bonte, De Wever ve Rots, 2010).

İnternet ortamında karşılaşılan tehditler arasında zararlı yazılımlar önemli bir yer tutmaktadır. Bu tür yazılımlar, bulaştıkları sistemlerde hem doğrudan teknik hasara yol açmakta hem de kullanıcıya ait verileri ele geçirerek dolaylı zararlar meydana getirmektedir. Program ve hizmetlerin işleyişini bozan virüsler, kendini çoğaltarak yayılan solucanlar ile zararsız içeriklerin içine gizlenerek sisteme sızan casus yazılımlar (truva atları ve keylogger türleri) zararlı yazılımlara örnek olarak gösterilebilir (Graham ve Howard, 2010). Bunun yanı sıra, internet kullanımında sıklıkla karşılaşılan tehditlerden biri de gizlilik ihlalleridir (Valcke vd., 2010). Kimlik numarası, iletişim bilgileri, adres ya da kredi kartı bilgileri gibi kişisel verilerin bilinçli ya da bilinçsiz biçimde üçüncü kişilerle paylaşılması, bireyler açısından ciddi güvenlik riskleri doğurabilmektedir.

Sosyal mühendislik teknikleri kullanılarak kimlik hırsızlığı ve dolandırıcılık vakaları görülebilmektedir (Garfinkel, 2012). Kimlik hırsızlığında yaygın olarak başvurulan yöntemlerden biri oltalama saldırılarıdır. Bu saldırılarda çoğunlukla sahte internet siteleri ya da yanıltıcı e-postalar kullanılmaktadır. Kullanıcı, bankadan ya da alışveriş yaptığı bir platformdan geldiğini düşündüğü mesajlara güvenerek kredi kartı veya çevrim içi bankacılık bilgilerini sahte bir web sayfasına girmekte ya da ilgili e-postaya yanıt vererek kişisel verilerini paylaşmaktadır. Mesajların güvenilirliğini artırmak amacıyla kurumlara ait logo ve kurumsal bilgiler taklit edilebilmektedir.

Ayrıca bilgisayarlara yetkisiz erişim sağlamak amacıyla kullanılan keylogger ve truva atı gibi zararlı yazılımlar da kimlik hırsızlığı süreçlerinde araç olarak kullanılabilmektedir. Bunun yanında internet kullanıcıları, çevrim içi ortamda siber zorbalık ve cinsel istismar gibi risklerle de karşı karşıya kalmaktadır. Siber zorbalık; bilgi ve iletişim teknolojileri aracılığıyla bir bireye ya da gruba yönelik olarak gerçekleştirilen, teknik ya da ilişkisel nitelikte zarar verme, aşağılayıcı söylemde bulunma ve olumsuz davranışlar sergileme biçimlerini kapsayan bir davranışlar bütünü olarak tanımlanmaktadır (Smith vd., 2008).

Bireysel siber güvenlik, kişinin kişisel verilerini, cihazlarını ve dijital kimliğini koruma amacıyla bilinçli ve güvenli davranışlar sergilemesini ifade eder (Erol vd., 2015). Bireylerin kurumsal sistemlerle olan etkileşimi arttıkça, güvenlik ihlallerine karşı bireysel sorumluluk da aynı oranda artmaktadır. Erol vd. (2015) tarafından geliştirilen Kişisel Siber Güvenliği Sağlama Ölçeği, bu bilinçli davranışları

ölçümleyen güvenilir bir araçtır. Ölçek, bireyin güvenli parola kullanımı, veri yedekleme, güncel yazılım kullanımı, sahte e-posta ayırt etme gibi davranışlarını kapsar.

Havacılık gibi yüksek güvenlik gerektiren sektörlerde, bireysel siber güvenlik davranışları kritik bir belirleyici olarak değerlendirilmektedir. Siber güvenlik yalnızca teknik bir konu değil; aynı zamanda bireylerin algıladıkları risk düzeyi ve sorumlulukları ile ilişkili bilişsel ve davranışsal bir süreçtir. Dijital ortamlarda karşılaşılan tehditlerin farkında olmak ve bu tehditlere karşı sürekli dikkatli davranma gerekliliği, bireylerin bilişsel yükünü artırabilmektedir. Özellikle teknoloji kullanımının yoğun olduğu iş ortamlarında, çalışanların güvenlik risklerine karşı daha hassas hale gelmeleri, sürekli dikkat ve kontrol gerektiren bir durum yaratarak stres düzeylerinin artmasıyla ilişkili olabilmektedir (Altıntaş ve Altıntaş, 2026; Altıntaş, Şanlı ve Odacı, 2026).

Bu bağlamda, bireysel siber güvenlik davranışlarının artmasının, bireylerin algıladıkları sorumluluk düzeyi ve risk farkındalığı üzerinden tekno-stres ile pozitif yönde ilişkili olabileceği değerlendirilmektedir. Dolayısıyla, bireysel siber güvenlik davranışlarının tekno-stres ile ilişkisi ve tekno-stresi yordama düzeyinin ampirik olarak incelenmesi önem arz etmektedir.

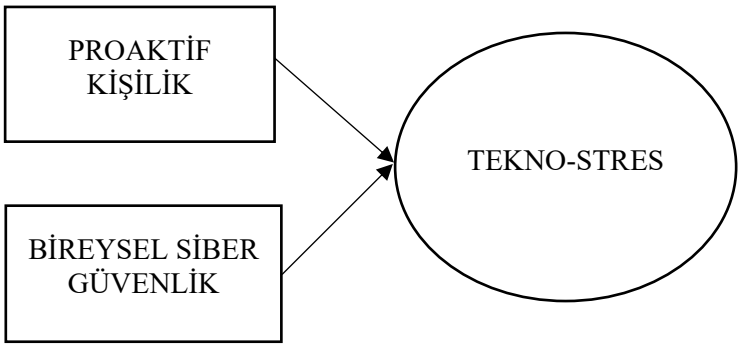
3. YÖNTEM

3.1. Araştırmanın Amacı, Modeli ve Hipotezler

Bu araştırmanın temel amacı, havacılık sektörü çalışanlarının proaktif kişilik özellikleri ve bireysel siber güvenlik davranışlarının tekno-stres düzeylerini yordama rollerini incelemektir. Bunun yanında, proaktif kişilik, bireysel siber güvenlik ve tekno-stres düzeylerinin katılımcıların demografik özelliklerine göre anlamlı farklılık gösterip göstermediği de değerlendirilmiştir. Araştırma, değişkenler arasındaki ilişkileri ve yordayıcı etkileri incelemeye yönelik ilişkisel tarama modeli kapsamında yapılandırılmıştır.

Çalışmada nicel araştırma yöntemi benimsenmiştir. Araştırma modeli, proaktif kişilik ve bireysel siber güvenlik değişkenlerinin tekno-stres üzerindeki etkisini birlikte değerlendirecek şekilde tasarlanmıştır. Kavramsal modelde proaktif kişilik ve bireysel siber güvenlik bağımsız değişkenler; tekno-stres ise bağımlı değişken olarak konumlandırılmıştır. Ayrıca cinsiyet, medeni durum, statü, yaş, eğitim düzeyi ve kurumda çalışma süresi gibi demografik değişkenler açısından araştırma değişkenlerinde anlamlı farklılık bulunup bulunmadığı da analiz edilmiştir.

Araştırmada değişkenler arasındaki ilişkileri belirlemek amacıyla korelasyon analizi; demografik değişkenlere göre farklılıkları incelemek amacıyla bağımsız örneklem t-testi, ANOVA, Welch testi, Games-Howell post-hoc karşılaştırmaları ve Kruskal–Wallis testi; proaktif kişilik ve bireysel siber güvenliğin tekno-stres üzerindeki yordayıcı etkisini belirlemek amacıyla ise çoklu doğrusal regresyon analizi kullanılmıştır. Araştırmanın hipotezleri doğrultusunda oluşturulan kavramsal model Şekil 1'de sunulmuştur.



Şekil 1. Araştırmaya Ait Kavramsal Model

Araştırmanın Hipotezleri;

H_1: Proaktif kişilik düzeyi, havacılık sektörü çalışanlarının tekno-stres düzeylerini negatif yönde ve anlamlı biçimde yordamaktadır.

H_2: Bireysel siber güvenlik davranış düzeyi, havacılık sektörü çalışanlarının tekno-stres düzeylerini pozitif yönde ve anlamlı biçimde yordamaktadır.

H_3: Havacılık sektörü çalışanlarının demografik özellikleri ile araştırma değişkenleri arasında anlamlı farklılıklar bulunmaktadır.

3.2. Evren ve Örneklem

Araştırmanın evrenini, Türkiye'de faaliyet gösteren kamu ve özel havacılık kurumlarında çalışan uçuş, teknik ve idari personel oluşturmaktadır. Örneklem, kolayda örnekleme yöntemi ve gönüllülük esasına dayalı olarak belirlenmiş olup araştırmaya toplam 387 çalışan katılmıştır. Bu kapsamda pilotlar, uçuş mürettebatı ve yer destek ekiplerinde görev yapan çalışanlar örnekleme dâhil edilmiştir.

Veriler, çevrim içi anket yöntemiyle toplanmış ve toplam 387 geçerli anket formu analize dâhil edilmiştir. Katılımcıların önemli bir kısmı aktif olarak uçuş operasyonlarında veya destek süreçlerinde görev yapmaktadır. Araştırma, değişkenler arasındaki ilişkilerin ve yordayıcı rollerin incelendiği ilişkisel bir araştırma deseni kapsamında yürütülmüştür.

Gürbüz ve Şahin'e (2014) göre, 100.000 kişilik bir evren için %95 güven düzeyinde gerekli örneklem büyüklüğü 383 olarak belirlenmiştir. Bu doğrultuda, araştırmada elde edilen 387 katılımcı sayısının evreni temsil etme ve istatistiksel analizler açısından yeterli olduğu değerlendirilmektedir.

Bu araştırmada kullanılan kolayda örnekleme ve gönüllülük esasına dayalı yaklaşım, hızlı veri toplama açısından avantaj sağlamakla birlikte, örneklemin temsiliyeti üzerinde belirli sınırlılıklar yaratmaktadır. Özellikle gönüllü katılıma dayalı veri toplama süreçlerinde, örgüte yönelik tutumları daha olumlu olan bireylerin araştırmaya katılma olasılığı daha yüksek olabilmektedir. Bu durum, literatürde öz-seçim yanlılığı olarak tanımlanan potansiyel bir örneklem yanlılığı riskini oluşturmaktadır.

Ayrıca araştırmada tüm verilerin öz-bildirim yoluyla toplanması nedeniyle ortak yöntem yanlılığı (common method bias) olasılığı Harman tek faktör testi ile kontrol edilmiştir. Bu amaçla, çalışmada kullanılan tüm ölçek maddeleri rotasyonsuz açıklayıcı faktör analizine tabi tutulmuştur. Analiz sonuçlarına göre, ilk faktörün açıkladığı toplam varyans oranının %50'nin altında kaldığı görülmüştür. Bu bulgu, çalışmada ortak yöntem yanlılığının ciddi bir tehdit oluşturmadığına işaret etmektedir. Bununla birlikte, Harman tek faktör testinin sınırlılıkları dikkate alındığında, elde edilen bulguların ihtiyatla yorumlanması önerilmektedir.

3.3. Veri Toplama Aracı

Çalışmanın etik kurul izni, İstanbul Gelişim Üniversitesi Rektörlüğü Etik Kurul Başkanlığı'nın 08.08.2025 tarihli, 2025-15 sayılı toplantısının 13 numaralı kararı ile alınmış olup veriler bu onay sonrasında toplanmıştır. Araştırma verileri, çevrim içi (Google Formlar) ve yüz yüze uygulanan anketler aracılığıyla toplam 387 katılımcıdan elde edilmiştir. Veri toplama aracı, dört bölümden oluşan yapılandırılmış bir anket formudur.

Demografik Bilgiler: Katılımcıların cinsiyet, yaş, eğitim durumu, statü, medeni durum ve sektör deneyimine ilişkin bilgilerden oluşmaktadır.

Proaktif Kişilik Ölçeği: Claes, Beheydt ve Lemmens (2005) tarafından geliştirilen ve Akın, Abacı, Kaya ve Arıcı (2011) tarafından Türkçeye uyarlanan kısa form esas alınmıştır. Ölçek, 10 maddeden oluşmaktadır. Ölçek, bireylerin inisiyatif alma, değişim yaratma ve çevresel koşulları etkileme eğilimlerini değerlendirmektedir.

Tekno-Stres Ölçeği: Tarafdar, Ragu-Nathan ve Ragu-Nathan (2007) tarafından geliştirilen ve Ilgaz, Özgür ve Çuhadar (2016) tarafından Türkçeye uyarlanan ölçek kullanılmıştır. Ölçek, 23 maddeden oluşmaktadır. Ölçek, bireylerin teknoloji kullanımına bağlı olarak yaşadıkları stres düzeyini tekno-aşırı yük, tekno-karmaşıklık ve tekno-belirsizlik gibi boyutlar çerçevesinde değerlendirmektedir.

Kişisel Siber Güvenlik Ölçeği: Erol, Şahin, Yılmaz ve Haseski (2015) tarafından geliştirilen ve bireylerin dijital güvenlik davranışlarını ölçen 25 maddelik ölçektir. Ölçek, bireylerin dijital ortamlarda güvenli davranış sergileme düzeylerini (güvenli parola kullanımı, veri koruma, tehdit farkındalığı vb.) ölçmektedir.

Bu çalışmada kavramsal olarak "bireysel siber güvenlik" ifadesi kullanılmış olup, ölçüm aracı olarak Erol vd. (2015) tarafından geliştirilen "Kişisel Siber Güvenlik Ölçeği"nden yararlanılmıştır. Tüm ölçek maddeleri 5'li Likert tipi (1 = Kesinlikle Katılmıyorum, 5 = Kesinlikle Katılıyorum) olarak yapılandırılmıştır.

Veri toplama süreci 10 Ekim 2025 – 31 Aralık 2025 tarihleri arasında yürütülmüştür. Bu süreçte toplam 389 anket formu toplanmış, eksik veri ve tutarsız işaretlemeler nedeniyle 2 anket analiz dışı bırakılmış ve 387 geçerli anket üzerinden analizler gerçekleştirilmiştir.

Katılımcıların gönüllülük esasına göre araştırmaya dâhil olması ve anketlerin hem çevrim içi hem yüz yüze uygulanması, erişilebilirliği artırmakla birlikte örneklemin temsiliyetine ilişkin sınırlılıkların tamamen ortadan kalkmadığını göstermektedir.

3.4. Verilerin Analizi

Araştırma kapsamında elde edilen veriler, SPSS 26 paket programı kullanılarak analiz edilmiştir. Analiz sürecinde öncelikle verilerin betimleyici özelliklerini belirlemek amacıyla frekans, yüzde, ortalama ve standart sapma değerleri hesaplanmıştır.

Verilerin normal dağılıma uygunluğu çarpıklık (skewness) ve basıklık (kurtosis) değerleri üzerinden değerlendirilmiştir. Bu değerlerin ±3 aralığında yer alması, normal dağılım varsayımı açısından kabul edilebilir sınırlar içinde değerlendirilmiştir. Ölçeklerin güvenirliğini belirlemek amacıyla Cronbach's Alpha katsayıları hesaplanmış ve elde edilen değerlerin kabul edilebilir düzeyde olduğu görülmüştür.

Ölçeklerin yapı geçerliliğine ilişkin destekleyici kanıt elde etmek amacıyla Kaiser-Meyer-Olkin (KMO) örneklem yeterliliği testi, Bartlett Küresellik Testi ve Açıklayıcı Faktör Analizi uygulanmıştır. Açıklayıcı Faktör Analizi kapsamında temel bileşenler yaklaşımı ve Varimax döndürme tekniği kullanılmıştır. Değişkenler arasındaki ilişkileri belirlemek amacıyla Pearson Korelasyon Analizi yapılmıştır.

Bu çalışmada kullanılan ölçekler daha önce farklı örneklemlerde geliştirilmiş ve uyarlanmış olmakla birlikte, mevcut örneklem grubunda yapı geçerliliğinin yeniden değerlendirilmesi amacıyla Açıklayıcı Faktör Analizi tercih edilmiştir. Doğrulayıcı faktör analizi daha güçlü bir geçerlilik kanıtı sunmakla birlikte, bu çalışmada keşfedici nitelikte bir yaklaşım benimsenmiş ve ölçeklerin mevcut örneklemdeki faktör yapısının ortaya konulması amaçlanmıştır.

Demografik değişkenlere göre araştırma değişkenlerinin farklılaşıp farklılaşmadığını belirlemek amacıyla bağımsız örneklem t-testleri, tek yönlü varyans analizi (ANOVA), Welch testi, Games-Howell post-hoc karşılaştırmaları ve Kruskal–Wallis testi kullanılmıştır. İki gruplu değişkenler olan cinsiyet ve medeni durum için bağımsız örneklem t-testi uygulanmıştır. İkiden fazla grup içeren statü, yaş, eğitim düzeyi ve kurumda çalışma süresi değişkenlerinde ise öncelikle Levene testi ile varyans homojenliği varsayımı incelenmiştir. Homojenlik varsayımının sağlandığı karşılaştırmalarda tek yönlü ANOVA ve Tukey HSD post-hoc testi; homojenlik varsayımının sağlanmadığı karşılaştırmalarda ise Welch testi ve Games-Howell post-hoc karşılaştırmaları dikkate alınmıştır. Yaş değişkeninde grup dağılımı ve varyans homojenliği sonuçları dikkate alınarak Kruskal–Wallis testi uygulanmıştır.

Bağımsız değişkenlerin bağımlı değişken üzerindeki yordayıcı rolünü belirlemek amacıyla çoklu doğrusal regresyon analizi yapılmıştır. Bu tercihin sebebi, bağımsız değişkenlerin tekno-stres üzerindeki özgül katkılarını birlikte değerlendirmektir. Bu analizde tekno-stres bağımlı değişken; proaktif kişilik ve bireysel siber güvenlik ise bağımsız değişkenler olarak modele dâhil edilmiştir. Regresyon analizinde çoklu doğrusal bağlantı varsayımı Tolerance ve VIF değerleriyle, artıklar arasındaki bağımsızlık ise Durbin-Watson katsayısıyla değerlendirilmiştir. Tüm istatistiksel analizlerde anlamlılık düzeyi $p < 0,05$ olarak kabul edilmiştir.

4. BULGULAR

Araştırmaya Türkiye'de faaliyet gösteren kamu ve özel havacılık kurumlarında görev yapan toplam 387 çalışan katılmıştır. Katılımcıların demografik özelliklerine ilişkin bulgular Tablo 1'de sunulmuştur.

Tablo 1. Demografik Bilgiler

Cinsiyet	**n**	**%**	**Medeni durum**	**n**	**%**
Kadın	188	48,6	Evli	171	44,2
Erkek	199	51,4	Bekâr	216	55,8
Yaş	**n**	**%**	**Kıdem**	**n**	**%**
18-23	78	20,2	1 yıldan az	104	26,9
24-33	135	34,9	1-5 yıl	183	47,3
34-43	76	19,6	6-10 yıl	48	12,4
44-58	94	24,3	11-20 yıl	40	10,3
59 ve üstü	4	1,0	21 yıl ve üzeri	12	3,1
Statü	**n**	**%**	**Eğitim**	**n**	**%**
Pilot	25	6,5	Lise	28	7,2
Uçuş Mürettebatı	22	5,7	Ön lisans	65	16,8
Yer Destek Ekibi	340	87,9	Lisans	212	54,8
			Lisansüstü	82	21,2

Tablo 1 incelendiğinde katılımcıların %51,4'ü erkek, %48,6'sı kadındır. Medeni durum açısından değerlendirildiğinde, katılımcıların %55,8'inin bekâr, %44,2'sinin evli olduğu belirlenmiştir.

Statü değişkenine göre, katılımcıların büyük çoğunluğunu yer destek personeli (%87,9) oluşturmaktadır. Bunu pilotlar (%6,5) ve uçuş mürettebatı (%5,7) izlemektedir. Statü dağılımında yer destek personelinin yüksek oranı, örneklemin operasyonel süreçlerde görev yapan çalışanlarda yoğunlaşmış olduğunu göstermektedir.

Yaş dağılımı incelendiğinde, 24–33 yaş aralığındaki katılımcıların %34,9 ile en büyük grubu oluşturduğu, bunu 44–58 yaş grubunun (%24,3) takip ettiği görülmektedir.

Eğitim düzeyi açısından katılımcıların %54,8'i lisans, %21,2'si lisansüstü, %16,8'i ön lisans ve %7,2'si lise mezunudur.

Kurumda çalışma süresi bakımından, katılımcıların %47,3'ünün 1–5 yıl, %26,9'unun ise 1 yıldan az kıdeme sahip olduğu belirlenmiştir.

Tablo 2. Normallik Testi Sonuçları

	Proaktif Kişilik	**Siber Güvenlik**	**Tekno-Stres**
Çarpıklık (Skewness)	-0,481	0,640	0,315
Basıklık (Kurtosis)	2,037	1,812	0,202

Tüm değişkenlere ait çarpıklık (skewness) ve basıklık (kurtosis) değerlerinin ±3 sınırları içerisinde yer aldığı görülmektedir. Bu durum, verilerin normal dağılıma yeterli düzeyde uyum sağladığını göstermektedir.

Özellikle proaktif kişilik ve siber güvenlik değişkenlerinin çarpıklık ve basıklık değerlerinin simetrik dağılıma yakın olduğu belirlenmiştir. Tekno-stres değişkenine ilişkin değerler de kabul edilebilir sınırlar içerisinde yer almaktadır.

Ölçeklere ilişkin verilerin -3 ile +3 aralığında olması, normallik varsayımının sağlandığını göstermektedir. Kalaycı (2010)'ya göre çarpıklık ve basıklık katsayılarının bu aralıkta yer alması, verilerin normal dağılım varsayımını karşıladığını ifade etmektedir.

Bu doğrultuda, araştırmada kullanılan ölçeklere ait verilerin normal dağılım gösterdiği kabul edilmiş ve analizlerde parametrik istatistiksel yöntemlerin kullanılmasının uygun olduğu sonucuna ulaşılmıştır.

Tablo 3. Ölçeklere Ait Güvenilirlik Analizleri

Proaktif Kişilik Ölçeği		Siber Güvenlik Ölçeği		Tekno-Stres Ölçeği	
Cronbach's Alpha	**n**	**Cronbach's Alpha**	**n**	**Cronbach's Alpha**	**n**
0,813	10	0,787	25	0,874	23

Araştırmada kullanılan üç ölçeğe ilişkin iç tutarlılık düzeylerini belirlemek amacıyla güvenilirlik analizleri yapılmış ve Cronbach's Alpha katsayıları hesaplanmıştır. Elde edilen bulgulara göre Cronbach's Alpha değeri; Proaktif Kişilik Ölçeği için 0,813, Kişisel Siber Güvenlik Ölçeği için 0,787 ve Tekno-Stres Ölçeği için 0,874 olarak bulunmuştur.

Literatürde Cronbach's Alpha katsayısının 0,70 ve üzerinde olması, ölçeklerin güvenilir kabul edilmesi için yeterli görülmektedir. Bu doğrultuda, Proaktif Kişilik Ölçeği ve Tekno-Stres Ölçeği yüksek düzeyde güvenilir, Kişisel Siber Güvenlik Ölçeği ise kabul edilebilir düzeyde güvenilir olarak değerlendirilmektedir. Özellikle Tekno-Stres Ölçeği'nin 0,874 gibi yüksek bir Cronbach's Alpha değerine sahip olması, ölçeğin maddeleri arasında güçlü bir iç tutarlılık bulunduğunu göstermektedir (Büyüköztürk, 2007).

Ölçeklerde yer alan madde sayıları incelendiğinde, Proaktif Kişilik Ölçeği'nin 10 madde, Kişisel Siber Güvenlik Ölçeği'nin 25 madde ve Tekno-Stres Ölçeği'nin 23 maddeden oluştuğu görülmektedir. Bu kapsamda, her üç ölçeğin de ölçmek istedikleri yapıları güvenilir biçimde değerlendirebilecek yeterli madde sayısına sahip olduğu söylenebilir.

Sonuç olarak, araştırmada kullanılan tüm ölçeklerin güvenilirlik düzeylerinin kabul edilebilir sınırların üzerinde olduğu, elde edilen verilerin istatistiksel analizler açısından güvenilir olduğu ve çalışmanın bulgularının sağlam ölçüm araçlarına dayandığı ifade edilebilir.

Tablo 4. KMO ve Bartlett's Testi

		Proaktif Kişilik	Siber Güvenlik	Tekno-Stres
Kaiser_Meyer_Olkin Measure of Sampling Adequacy.		0,765	0,811	0,760
Bartlett's-Test of-Sphericity	**Approx. Chi.Square**	1299,20	5797,75	4537,86
	Df	45	300	253
	Sig.	0,000	0,000	0,000

Araştırmada kullanılan veri seti, Proaktif Kişilik Ölçeği, Kişisel Siber Güvenlik Ölçeği ve Tekno-Stres Ölçeği olmak üzere üç ana ölçüm aracından oluşmaktadır. Ölçeklerin güvenilirlik düzeyleri Cronbach's Alpha katsayılarıyla incelenmiş; yapı geçerliliğine ilişkin destekleyici kanıt elde etmek amacıyla ise sonrasında Açıklayıcı Faktör Analizi uygulanmıştır. Analiz öncesinde araştırmada kullanılan ölçeklerin faktör analizine uygunluğunu değerlendirmek amacıyla Kaiser-Meyer-Olkin (KMO) örneklem yeterliliği testi ve Bartlett's Küresellik Testi uygulanmış ve elde edilen bulgular, verilerin faktör analizine uygun olduğunu göstermiştir.

Elde edilen sonuçlara göre, Proaktif Kişilik Ölçeği için Kaiser-Meyer-Olkin (KMO) değeri 0,765, Kişisel Siber Güvenlik Ölçeği için 0,811 ve Tekno-Stres Ölçeği için 0,760 olarak belirlenmiştir. Literatürde Kaiser-Meyer-Olkin (KMO) değerinin 0,50'nin üzerinde olması faktör analizi için yeterli kabul edilmekte; 0,60–0,80 arası değerler iyi, 0,80 ve üzeri değerler ise çok iyi örneklem yeterliliğine işaret etmektedir (Kalaycı, 2014). Bu doğrultuda elde edilen KMO değerleri, ölçeklerin faktör analizi için uygun olduğunu göstermektedir. Bartlett's Küresellik Testi sonuçlarına göre tüm ölçeklerde anlamlılık düzeyi $p < 0,001$ olarak bulunmuştur. Bu sonuç, maddeler arasında istatistiksel olarak anlamlı korelasyonlar bulunduğunu ve verilerin faktör analizine elverişli olduğunu göstermektedir.

Proaktif Kişilik Ölçeği, Claes, Beheydt ve Lemmens (2005) tarafından geliştirilen ve Akın, Abacı, Kaya ve Arıcı (2011) tarafından Türkçeye uyarlanan kısa form esas alınarak kullanılmıştır. Bu çalışmada ölçeğin Kaiser-Meyer-Olkin (KMO) değeri 0,765 olarak belirlenmiş, Bartlett's Küresellik Testi sonucu ise istatistiksel olarak anlamlı bulunmuştur ($\chi^2 = 1299,20$; df = 45; $p < 0,001$). Açıklayıcı Faktör Analizi sonucunda özdeğeri 1'in üzerinde olan üç faktörlü bir yapı elde edilmiştir. Bu yapı toplam varyansın %65,01'ini açıklamaktadır. Maddelerin ortak varyans değerlerinin kabul edilebilir düzeyde olması ve faktör yüklerinin genel olarak güçlü görünmesi nedeniyle ölçekten herhangi bir madde çıkarılmamıştır. Bu bulgular, Proaktif Kişilik Ölçeği'nin araştırma örnekleminde yapı geçerliliği açısından yeterli düzeyde desteklendiğini göstermektedir.

Kişisel Siber Güvenlik Ölçeği, Erol, Şahin, Yılmaz ve Haseski (2015) tarafından geliştirilen ve bireylerin dijital güvenlik davranışlarını ölçmeyi amaçlayan 25 maddelik bir ölçektir. Bu araştırmada kavramsal olarak "bireysel siber güvenlik" ifadesi kullanılmış; ölçüm aracı olarak ise söz konusu ölçekten yararlanılmıştır. Ölçeğe ilişkin Kaiser-Meyer-Olkin (KMO) değeri 0,811 olarak hesaplanmış, Bartlett's Küresellik Testi sonucu da anlamlı bulunmuştur ($\chi^2 = 5797,75$; df = 300; $p < 0,001$). Açıklayıcı Faktör Analizi sonucunda altı faktörlü bir yapı elde edilmiş ve bu yapı toplam varyansın %69,09'unu açıklamıştır. Açıklanan varyans oranının yüksek olması, maddelerin ortak varyans değerlerinin genel olarak yeterli düzeyde bulunması ve ölçeğin güvenilirlik katsayısının kabul edilebilir sınırlar içinde yer alması, Kişisel Siber Güvenlik Ölçeği'nin yapı geçerliliğine ilişkin güçlü destekleyici kanıtlar sunduğunu göstermektedir.

Tekno-Stres Ölçeği, Tarafdar, Ragu-Nathan ve Ragu-Nathan (2007) tarafından geliştirilen ve Ilgaz, Özgür ve Çuhadar (2016) tarafından Türkçeye uyarlanan ölçüm aracı esas alınarak kullanılmıştır. Ölçeğin Kaiser-Meyer-Olkin (KMO) değeri 0,760 olarak bulunmuş, Bartlett's Küresellik Testi sonucu ise istatistiksel olarak anlamlı çıkmıştır ($\chi^2 = 4537,86$; df = 253; $p < 0,001$). Açıklayıcı Faktör Analizi sonucunda özdeğeri 1'in üzerinde olan beş faktörlü bir yapı ortaya çıkmıştır. Bu yapı toplam varyansın %62,83'ünü açıklamaktadır. Tekno-stresin literatürde çok boyutlu bir yapı olarak ele alınması dikkate alındığında, elde edilen beş faktörlü yapı kuramsal açıdan da anlamlı görünmektedir. Ortak varyans değerlerinin kabul edilebilir düzeyde olması ve ölçeğin yüksek iç tutarlılık katsayısına sahip bulunması nedeniyle herhangi bir madde çıkarılmamıştır. Bu sonuçlar, Tekno-Stres Ölçeği'nin araştırma örnekleminde yapı geçerliliği açısından yeterli düzeyde desteklendiğine işaret etmektedir.

Elde edilen bulgular birlikte değerlendirildiğinde, araştırmada kullanılan üç ölçeğin de faktör analizine uygun veri yapısına sahip olduğu ve Açıklayıcı Faktör Analizi sonuçlarının yapı geçerliliğini desteklediği görülmektedir. Proaktif Kişilik Ölçeği toplam varyansın %65,01'ini, Kişisel Siber Güvenlik Ölçeği %69,09'unu ve Tekno-Stres Ölçeği %62,83'ünü açıklamıştır. Bu oranlar sosyal bilimler alanında kabul edilebilir düzeyin üzerinde değerlendirilebilir. Araştırmanın temel modelinde proaktif kişilik, bireysel siber güvenlik ve tekno-stres değişkenleri bütüncül yapılar olarak ele alındığından, sonraki analizlerde ölçeklerin toplam puanları kullanılmıştır. Bu yönüyle araştırmada kullanılan ölçüm araçlarının güvenilirlik ve yapı geçerliliği açısından yeterli kanıt sunduğu söylenebilir.

Tablo 5. T testi (Cinsiyet, Medeni durum)

Cinsiyet		**N**	**M**	**S.S.**	**p**
Proaktif Kişilik	Kadın	188	3,93	,39	< ,001
	Erkek	199	3,73	,48	
Siber Güvenlik	Kadın	188	3,12	,32	,651
	Erkek	199	3,10	,36	
Tekno-Stres	Kadın	188	2,84	,53	,401
	Erkek	199	2,88	,53	
Medeni durum		**N**	**M**	**S.S.**	p
Proaktif Kişilik	Evli	171	3,66	,47	< ,001
	Bekâr	216	3,97	,38	
Siber Güvenlik	Evli	171	3,03	,30	< ,001
	Bekâr	216	3,17	,36	
Tekno-Stres	Evli	171	2,89	,50	,277
	Bekâr	216	2,83	,55	

Bağımsız örneklem t-testi ile araştırma değişkenlerinin cinsiyet ve medeni duruma göre farklılaşıp farklılaşmadığı incelenmiştir.

Cinsiyete göre proaktif kişilik puanlarının kadınlarda (M = 3,93; SS = 0,39) erkeklere kıyasla (M = 3,73; SS = 0,48) anlamlı düzeyde daha yüksek olduğu belirlenmiştir (p < ,001). Buna karşın siber güvenlik (kadın: M = 3,12; SS = 0,32; erkek: M = 3,10; SS = 0,36; p = ,651) ve tekno-stres (kadın: M = 2,84; SS = 0,53; erkek: M = 2,88; SS = 0,53; p = ,401) puanlarının cinsiyete göre anlamlı biçimde farklılaşmadığı görülmüştür. Bu sonuçlara göre, cinsiyet değişkeni yalnızca proaktif kişilik üzerinde anlamlı bir farklılık oluşturmakta, ancak siber güvenlik ve tekno-stres düzeylerinde anlamlı bir farklılık göstermemektedir.

Medeni duruma göre yapılan analizlerde, proaktif kişilik puanlarının bekâr çalışanlarda (M = 3,97; SS = 0,38) evli çalışanlara kıyasla (M = 3,66; SS = 0,47) anlamlı düzeyde daha yüksek olduğu belirlenmiştir (p < ,001). Benzer şekilde siber güvenlik puanlarının da bekâr çalışanlarda (M = 3,17; SS = 0,36) evli çalışanlara göre (M = 3,03; SS = 0,30) anlamlı biçimde daha yüksek olduğu görülmüştür (p < ,001). Tekno-stres puanlarının ise medeni duruma göre anlamlı farklılık göstermediği belirlenmiştir (evli: M=2,89; SS=0,50; bekâr: M=2,83; SS=0,55; p = ,277). Bu bulgular, medeni durumun proaktif kişilik ve siber güvenlik üzerinde anlamlı bir farklılık oluşturduğunu, ancak tekno-stres düzeyleri üzerinde anlamlı bir farklılık göstermediğini açıklamaktadır.

Çok gruplu karşılaştırmalara geçilmeden önce bağımlı değişkenlere ilişkin gruplar arası varyansların homojenliği Levene testi ile incelenmiştir. Levene testi sonuçları, bazı karşılaştırmalarda varyans homojenliği varsayımının sağlandığını, bazı karşılaştırmalarda ise bu varsayımın karşılanmadığını göstermiştir. Bu nedenle homojenlik varsayımının sağlandığı karşılaştırmalarda tek yönlü ANOVA ve Tukey HSD post-hoc testi; homojenlik varsayımının sağlanmadığı karşılaştırmalarda ise Welch testi ve Games-Howell post-hoc karşılaştırmaları dikkate alınmıştır. Yaş değişkeninde ise grup dağılımı ve varyans homojenliği sonuçları dikkate alınarak Kruskal–Wallis testi uygulanmıştır. Katılımcıların statü, yaş, eğitim düzeyi ve kurumda çalışma süresi değişkenlerine göre proaktif kişilik, bireysel siber güvenlik ve tekno-stres düzeylerinin farklılaşıp farklılaşmadığını belirlemek amacıyla yapılan karşılaştırma analizlerine ilişkin sonuçlar Tablo 6'da sunulmaktadır.

Tablo 6. Demografik Değişkenlere Göre Karşılaştırma Testi Sonuçları (Statü, Yaş, Eğitim, Kıdem)

Demografik Değişken	Ölçek	Kullanılan Test	Test Değeri	df	p	Sonuç	Post-hoc / Karşılaştırma
Statü	Tekno-Stres	Welch	16,426	2; 39,008	<0,001	Anlamlı fark var	Uçuş mürettebatı > Pilot; Uçuş mürettebatı > Yer destek ekibi
	Bireysel Siber Güvenlik	Welch	64,482	2; 53,573	<0,001	Anlamlı fark var	Uçuş mürettebatı > Pilot; Uçuş mürettebatı > Yer destek ekibi; Yer destek ekibi > Pilot
	Proaktif Kişilik	ANOVA	3,588	2; 384	0,029	Anlamlı fark var	Uçuş mürettebatı > Pilot
Yaş	Tekno-Stres	Kruskal–Wallis	H = 5,385	4	0,250	Anlamlı fark yok	-
	Bireysel Siber Güvenlik	Kruskal–Wallis	H = 29,374	4	<0,001	Anlamlı fark var	18–23 yaş grubu en yüksek sıra ortalamasına sahiptir
	Proaktif Kişilik	Kruskal–Wallis	H = 7,094	4	0,131	Anlamlı fark yok	-
Eğitim	Tekno-Stres	Welch	6,068	3; 89,696	0,001	Anlamlı fark var	Lisansüstü > Ön lisans; Lisansüstü > Lisans
	Bireysel Siber Güvenlik	Welch	1,663	3; 109,339	0,179	Anlamlı fark yok	-
	Proaktif Kişilik	Welch	15,089	3; 93,472	<0,001	Anlamlı fark var	Ön lisans > Lise; Ön lisans > Lisans; Ön

							lisans > Lisansüstü
Kıdem	Tekno-Stres	Welch	16,988	4; 69,171	<0,001	Anlamlı fark var	11–20 yıl > 1 yıldan az, 1–5 yıl, 6–10 yıl; 21 yıl ve üzeri > 1 yıldan az, 1–5 yıl
	Bireysel Siber Güvenlik	Welch	7,414	4; 87,550	<0,001	Anlamlı fark var	1 yıldan az > 1–5 yıl; 11–20 yıl > 1–5 yıl
	Proaktif Kişilik	Welch	4,926	4; 78,136	0,001	Anlamlı fark var	1 yıldan az > 11–20 yıl

Not: Homojenlik varsayımının sağlandığı karşılaştırmalarda ANOVA ve Tukey HSD; homojenlik varsayımının sağlanmadığı karşılaştırmalarda Welch testi ve Games-Howell post-hoc karşılaştırmaları dikkate alınmıştır. Yaş değişkenine ilişkin karşılaştırmalarda Kruskal–Wallis testi uygulanmıştır.

* $p < 0,05$.

Analiz bulgularına göre statü değişkeni açısından proaktif kişilik, bireysel siber güvenlik ve tekno-stres değişkenlerinde anlamlı farklılıklar tespit edilmiştir. Tekno-stres açısından uçuş mürettebatının pilotlar ve yer destek personeline göre daha yüksek ortalamaya sahip olduğu görülmektedir. Bireysel siber güvenlik düzeyi açısından da uçuş mürettebatının diğer gruplara göre daha yüksek puan aldığı; yer destek personelinin ise pilotlardan daha yüksek ortalamaya sahip olduğu belirlenmiştir. Proaktif kişilik açısından ise uçuş mürettebatının pilotlara göre daha yüksek puan aldığı görülmektedir. Bu bulgular, görev türü ve operasyonel sorumluluk farklılıklarının çalışanların teknolojiyle ilişkili stres, güvenlik davranışı ve proaktif eğilimleri ile ilişkili olabileceğini göstermektedir.

Yaş değişkenine ilişkin Kruskal–Wallis testi sonuçları, tekno-stres ve proaktif kişilik düzeylerinin yaş gruplarına göre anlamlı biçimde farklılaşmadığını göstermektedir. Buna karşılık bireysel siber güvenlik değişkeninde yaş grupları arasında anlamlı farklılık tespit edilmiştir. Sıra ortalamaları incelendiğinde, 18–23 yaş grubunun bireysel siber güvenlik düzeyinin diğer yaş gruplarına göre daha yüksek olduğu görülmektedir. Bu sonuç, genç çalışanların dijital güvenlik davranışlarının daha yüksek düzeyde olduğunu göstermektedir.

Eğitim düzeyi açısından tekno-stres ve proaktif kişilik değişkenlerinde anlamlı farklılıklar belirlenmiştir. Tekno-stres düzeyinin lisansüstü mezunlarında ön lisans ve lisans mezunlarına göre daha yüksek olduğu görülmektedir. Proaktif kişilik açısından ise ön lisans mezunlarının lise, lisans ve lisansüstü mezunlarına kıyasla daha yüksek ortalamaya sahip olduğu belirlenmiştir. Bireysel siber güvenlik değişkeninde ise eğitim düzeyine göre anlamlı bir farklılık saptanmamıştır. Bu bulgular, eğitim düzeyinin özellikle tekno-stres ve proaktif kişilik üzerinde farklılaştırıcı bir rol oynadığını göstermektedir.

Kurumda çalışma süresi (kıdem) açısından üç değişkende de anlamlı farklılık bulunmuştur. Tekno-stres düzeyinin 11–20 yıl ve 21 yıl ve üzeri kıdeme sahip çalışanlarda daha yüksek olduğu görülmektedir. Bireysel siber güvenlik açısından 1 yıldan az ve 11–20 yıl kıdeme sahip çalışanların 1–5 yıl kıdeme sahip çalışanlara göre daha yüksek ortalamalara sahip olduğu belirlenmiştir. Proaktif kişilikte ise 1 yıldan az kıdeme sahip çalışanların 11–20 yıl kıdeme sahip çalışanlara göre daha yüksek puan aldığı görülmektedir. Bu bulgular, kurumda çalışma süresinin özellikle tekno-stres üzerinde anlamlı farklılık oluşturduğunu göstermektedir.

Bu bulgular birlikte değerlendirildiğinde, demografik değişkenlerin proaktif kişilik, bireysel siber güvenlik ve tekno-stres üzerinde kısmi farklılıklar oluşturduğu söylenebilir. Statü, eğitim düzeyi ve kurumda çalışma süresi bazı değişkenlerde anlamlı farklılık gösterirken, yaş değişkeni yalnızca bireysel siber güvenlik açısından anlamlı bir farklılık ortaya koymuştur. Bu nedenle H_3 hipotezi kısmen kabul edilmiştir.

Tablo 7. Değişkenler Arasında Korelasyon Analizi

		Proaktif Kişilik	Siber Güvenlik	Tekno-Stres
Proaktif Kişilik	**Pearson C.**	1		
	Sig. (2)			
	N	387		
Siber Güvenlik	**Pearson C.**	0,19**	1	
	Sig. (2)	< ,001		
	N	387	387	
Tekno-Stres	**Pearson C.**	-0,16**	0,49**	1
	Sig. (2)	< ,001	< ,001	
	N	387	387	387

Proaktif kişilik, siber güvenlik ve tekno-stres değişkenleri arasındaki ilişkilerin belirlenmesi amacıyla Pearson korelasyon analizi yapılmıştır. Korelasyon katsayısı "r" ile ifade edilmekte olup -1 ile +1 arasında değer alabilmektedir (Gürbüz ve Şahin, 2014). Analiz sonuçlarına göre değişkenler arasında istatistiksel olarak anlamlı ilişkiler bulunmaktadır (N = 387).

Proaktif kişilik ile bireysel siber güvenlik arasında pozitif yönlü, düşük düzeyde ve anlamlı bir ilişki tespit edilmiştir (r = ,19, p < ,01). Bu bulgu, proaktif kişilik düzeyi ile bireysel siber güvenlik davranışları arasında aynı yönlü bir ilişki olduğunu göstermektedir. Başka bir ifadeyle bulgu, bireylerin; girişimci, sorumluluk almaya yatkın ve inisiyatif kullanabilme davranışları ile dijital ortamlarda güvenli davranış sergileme davranışlarının ilişkili olabileceğine işaret etmektedir.

Proaktif kişilik ile tekno-stres arasında düşük düzeyde, negatif yönlü ve anlamlı bir ilişki bulunmaktadır (r = -0,16, p < ,01). Bu sonuç, proaktif kişilik düzeyi ile tekno-stres arasında ters yönlü bir ilişki olduğunu göstermektedir. Proaktif bireylerin değişime daha açık olmaları, problem çözme becerilerinin gelişmiş olması ve teknolojiye daha hızlı uyum sağlamaları, tekno-stresle başa çıkabilmelerine katkı sağlamaktadır. Proaktif bireyler böylelikle, teknolojiye daha hazırlıklı ve kontrollü yaklaşarak stres seviyelerini düşük tutabilirler.

Bireysel siber güvenlik ile tekno-stres arasında ise pozitif yönlü, orta düzeyde ve anlamlı bir ilişki bulunmaktadır (r = ,49, p < ,001). Bu bulgu, bireysel siber güvenlik davranışları ile tekno-stres düzeyi arasında aynı yönlü bir ilişki olduğunu göstermektedir. Özellikle siber tehditler, veri güvenliği ve dijital riskler konusunda daha bilinçli olan bireylerin, bu risklere karşı daha hassas hale gelmeleri, teknoloji kullanım sürecinde stres düzeylerinin yükselmesi ile ilişkili olabilmektedir.

Regresyon analizinin temel amacı, bağımsız değişkenlerin bağımlı değişken üzerindeki yordayıcı etkilerini belirlemektir. Bu çalışmada, proaktif kişilik ve bireysel siber güvenlik değişkenlerinin tekno-stres üzerindeki özgül yordayıcı katkılarını birlikte değerlendirmek amacıyla çoklu doğrusal regresyon analizi uygulanmıştır. Bu analizde tekno-stres bağımlı değişken; bireysel siber güvenlik ve proaktif kişilik ise bağımsız değişkenler olarak modele dâhil edilmiştir. Çoklu doğrusal bağlantı varsayımı Tolerance ve VIF değerleri üzerinden incelenmiş; artıklar arasındaki bağımsızlık ise Durbin-Watson katsayısı ile değerlendirilmiştir. Analiz sonuçları Tablo 8'de sunulmaktadır.

Tablo 8. Çoklu Doğrusal Regresyon Analizi

Bağımlı Değişken	Bağımsız Değişken	B	Std. Hata	β	t	p	Tolerance	VIF
Tekno-Stres	Sabit	1,450	0,257	-	5,638	<0,001	-	-
	Bireysel Siber Güvenlik	0,836	0,067	0,541	12,509	<0,001	0,964	1,037
	Proaktif Kişilik	-0,311	0,051	-0,265	-6,123	<0,001	0,964	1,037

Model özeti: R = 0,555; R^2 = 0,308; Düzeltilmiş R^2 = 0,305; F(2,384) = 85,529; p < 0,001; Durbin-Watson = 1,809.

Çoklu doğrusal regresyon analizi sonucunda kurulan modelin istatistiksel olarak anlamlı olduğu belirlenmiştir ($F(2,384) = 85,529$; $p < 0,001$). Modelin açıklayıcılık düzeyi incelendiğinde, proaktif kişilik ve bireysel siber güvenlik değişkenlerinin birlikte tekno-stres düzeyindeki toplam varyansın yaklaşık %30,8'ini açıkladığı görülmektedir ($R^2 = 0,308$; Düzeltilmiş $R^2 = 0,305$). Bu oran, modelin tekno-stres düzeyini açıklamada dikkate değer (orta düzeyde) bir açıklayıcılığa sahip olduğunu göstermektedir.

Çoklu doğrusal bağlantı varsayımı incelendiğinde, her iki bağımsız değişken için Tolerance değerinin 0,964 ve VIF değerinin 1,037 olduğu görülmektedir. Tolerance değerlerinin 0,10'un üzerinde, VIF değerlerinin ise 10'un oldukça altında olması, modelde çoklu doğrusal bağlantı sorunu bulunmadığını göstermektedir. Ayrıca Durbin-Watson değerinin 1,809 olarak hesaplanması, artıklar arasında otokorelasyon açısından önemli bir sorun bulunmadığına işaret etmektedir.

Bağımsız değişkenlere ilişkin katsayılar incelendiğinde, bireysel siber güvenliğin tekno-stres üzerinde pozitif yönlü ve anlamlı bir yordayıcı olduğu görülmektedir ($B = 0,836$; $\beta = 0,541$; $t = 12,509$; $p < 0,001$). Bu bulgu, bireysel siber güvenlik düzeyi ile tekno-stres arasında aynı yönlü bir ilişki bulunduğunu ve bireysel siber güvenliğin tekno-stresin anlamlı bir yordayıcısı olduğunu göstermektedir. Bulgu, dijital güvenlik farkındalığı ve güvenlik prosedürlerine yönelik duyarlılığın çalışanlarda daha yüksek teknoloji kaynaklı stres algısıyla birlikte seyredebileceğine işaret etmektedir. Bu sonuç, siber güvenlik davranışlarının yalnızca koruyucu bir unsur olarak değil; risk algısı, dikkat yükü ve prosedürel sorumluluk üzerinden tekno-stresle ilişkili bir değişken olarak da değerlendirilmesi gerektiğini düşündürmektedir.

Proaktif kişilik değişkeninin ise tekno-stres üzerinde negatif ve anlamlı bir yordayıcı olduğu belirlenmiştir ($B = -0,311$; $\beta = -0,265$; $t = -6,123$; $p < 0,001$). Bu sonuç, proaktif kişilik ile tekno-stres arasında ters yönlü bir ilişki bulunduğunu ve proaktif kişiliğin tekno-stresin anlamlı bir yordayıcısı olduğunu göstermektedir. Proaktif bireylerin değişime daha hızlı uyum sağlama, sorunları önceden fark etme, çözüm üretme ve teknolojiyle ilişkili belirsizlikleri daha yönetilebilir algılama eğilimleri, bu negatif ilişkiyi açıklayabilecek olası mekanizmalar arasında değerlendirilebilir.

Standartlaştırılmış beta katsayıları birlikte değerlendirildiğinde, bireysel siber güvenliğin tekno-stres üzerindeki yordayıcı etkisinin proaktif kişiliğe göre daha güçlü olduğu görülmektedir. Bu durum, model içerisinde bireysel siber güvenliğin göreli öneminin daha yüksek olduğunu göstermektedir. Bireysel siber güvenlik pozitif yönde daha yüksek bir etki sergilerken, proaktif kişilik tekno-stresi azaltıcı yönde anlamlı fakat görece daha düşük düzeyde bir katkı sunmaktadır. Bu bulgu, tekno-stresin yalnızca bireysel başa çıkma eğilimleriyle değil, aynı zamanda dijital güvenlik sorumlulukları ve risk farkındalığıyla da yakından ilişkili olabileceğini göstermektedir.

Bu doğrultuda, proaktif kişilik düzeyinin tekno-stresi negatif yönde ve anlamlı biçimde yordadığı; bireysel siber güvenlik düzeyinin ise tekno-stresi pozitif yönde ve anlamlı biçimde yordadığı belirlenmiştir. Bu bulgular doğrultusunda, proaktif kişilik ve bireysel siber güvenlik değişkenlerinin tekno-stresin anlamlı yordayıcıları olduğu belirlenmiştir. Bu nedenle H_1 ve H_2 hipotezleri kabul edilmiştir.

Tablo 9. Hipotez Sonuçları

Hipotez	**Sonuç**
H_1: Proaktif kişilik düzeyi, havacılık sektörü çalışanlarının tekno-stres düzeylerini negatif yönde ve anlamlı biçimde yordamaktadır.	**Kabul**
H_2: Bireysel siber güvenlik davranış düzeyi, havacılık sektörü çalışanlarının tekno-stres düzeylerini pozitif yönde ve anlamlı biçimde yordamaktadır.	**Kabul**
H_3: Havacılık sektörü çalışanlarının demografik özellikleri ile araştırma değişkenleri arasında anlamlı farklılıklar bulunmaktadır.	**Kısmen Kabul**

Not: Hipotez sonuçları, çoklu doğrusal regresyon ve grup karşılaştırma analizlerinden elde edilen bulgular doğrultusunda değerlendirilmiştir.

Araştırmada test edilen H_1 hipotezi, proaktif kişilik düzeyinin havacılık sektörü çalışanlarının tekno-stres düzeyleri üzerindeki yordayıcı rolünü incelemektedir. Yapılan çoklu doğrusal regresyon analizi sonucunda, proaktif kişiliğin tekno-stres üzerinde negatif yönlü ve anlamlı bir yordayıcı olduğu belirlenmiştir ($\beta = -0{,}265$; $p < 0{,}001$). Bu bulgu, bireysel siber güvenlik değişkeniyle birlikte modele dâhil edildiğinde de proaktif kişiliğin tekno-stresi azaltıcı yönde anlamlı bir katkı sunduğunu göstermektedir. Elde edilen sonuç, proaktif kişilik ile tekno-stres arasında ters yönlü bir ilişki bulunduğunu ortaya koymaktadır. Bu durum, proaktif bireylerin teknolojik değişimlere daha hızlı uyum sağlama, karşılaştıkları sorunlara çözüm odaklı yaklaşma ve belirsizlikleri daha yönetilebilir algılama eğilimleriyle açıklanabilir. Bu doğrultuda "H_1: Proaktif kişilik düzeyi, havacılık sektörü çalışanlarının tekno-stres düzeylerini negatif yönde ve anlamlı biçimde yordamaktadır." hipotezi kabul edilmiştir.

Araştırmada test edilen H_2 hipotezi, bireysel siber güvenlik davranış düzeyinin havacılık sektörü çalışanlarının tekno-stres düzeyleri üzerindeki yordayıcı rolünü incelemektedir. Çoklu doğrusal regresyon analizi sonucunda bireysel siber güvenliğin tekno-stres üzerinde pozitif yönlü ve anlamlı bir yordayıcı olduğu tespit edilmiştir ($\beta = 0{,}541$; $p < 0{,}001$). Bu bulgu, proaktif kişilik değişkeni kontrol edildiğinde dahi bireysel siber güvenlik davranışlarının tekno-stres üzerinde güçlü açıklayıcılığı olan anlamlı bir katkı sunduğunu göstermektedir. Elde edilen sonuç, bireysel siber güvenlik ile tekno-stres arasında aynı yönlü bir ilişki bulunduğuna işaret etmektedir. Buna göre, siber güvenlik konusunda daha duyarlı olan çalışanların güvenlik risklerini daha yoğun algılamaları, prosedürlere uyum konusunda daha fazla dikkat göstermeleri ve dijital tehditlere karşı sürekli tetikte olmaları, tekno-stres düzeylerinin artmasıyla ilişkili olabilir. Dolayısıyla bireysel siber güvenlik davranışları yalnızca koruyucu bir unsur olarak değil, aynı zamanda risk algısı ve dikkat yükü üzerinden tekno-stresle ilişkili bir değişken olarak değerlendirilebilir. Bu doğrultuda "H_2: Bireysel siber güvenlik davranış düzeyi, havacılık sektörü çalışanlarının tekno-stres düzeylerini pozitif yönde ve anlamlı biçimde yordamaktadır." hipotezi kabul edilmiştir.

Bağımsız örneklem t-testi sonuçlarına göre cinsiyet değişkeni yalnızca proaktif kişilik düzeyinde anlamlı farklılık oluşturmuştur. Kadın katılımcıların proaktif kişilik ortalaması erkek katılımcılara göre daha yüksek bulunmuştur. Buna karşılık bireysel siber güvenlik ve tekno-stres düzeyleri cinsiyete göre anlamlı biçimde farklılaşmamaktadır. Medeni durum açısından ise proaktif kişilik ve bireysel siber güvenlik değişkenlerinde anlamlı farklılık tespit edilmiş; bekâr çalışanların her iki değişkende de evli çalışanlara göre daha yüksek ortalamalara sahip olduğu görülmüştür. Tekno-stres düzeyi ise medeni duruma göre anlamlı bir farklılık göstermemiştir.

Statü değişkeni açısından yapılan karşılaştırma analizlerinde proaktif kişilik, bireysel siber güvenlik ve tekno-stres değişkenlerinde anlamlı farklılıklar belirlenmiştir. Tekno-stres açısından uçuş mürettebatının pilotlar ve yer destek ekibine göre daha yüksek ortalamaya sahip olduğu görülmektedir. Bireysel siber güvenlik düzeyinde de uçuş mürettebatı diğer gruplara kıyasla daha yüksek puan almıştır. Proaktif kişilik açısından ise uçuş mürettebatının pilotlara göre daha yüksek düzeyde olduğu belirlenmiştir. Bu bulgular, görev türü ve operasyonel sorumluluk farklılıklarının çalışanların teknolojiyle ilişkili stres, güvenlik davranışı ve proaktif eğilimleri üzerinde etkili olabileceğini düşündürmektedir.

Yaş değişkenine ilişkin Kruskal–Wallis testi sonuçları, tekno-stres ve proaktif kişilik düzeylerinin yaş gruplarına göre anlamlı biçimde farklılaşmadığını göstermektedir. Buna karşılık bireysel siber güvenlik düzeylerinde yaş grupları arasında anlamlı farklılık tespit edilmiştir. Sıra ortalamaları incelendiğinde, 18–23 yaş grubunun bireysel siber güvenlik düzeyinin diğer yaş gruplarına göre daha yüksek olduğu görülmektedir. Bu bulgu, genç çalışanların dijital güvenlik davranışları bakımından daha duyarlı bir görünüm sergileyebileceğine işaret etmektedir.

Eğitim düzeyi açısından tekno-stres ve proaktif kişilik değişkenlerinde anlamlı farklılıklar belirlenmiştir. Tekno-stres düzeyinin lisansüstü mezunlarında ön lisans ve lisans mezunlarına göre daha yüksek olduğu görülmektedir. Proaktif kişilik açısından ise ön lisans mezunlarının lise, lisans ve lisansüstü mezunlarına kıyasla daha yüksek ortalamaya sahip olduğu belirlenmiştir. Bireysel siber güvenlik değişkeninde ise eğitim düzeyine göre anlamlı bir farklılık saptanmamıştır. Bu nedenle eğitim düzeyinin özellikle tekno-stres ve proaktif kişilik üzerinde farklılaştırıcı bir rol oynadığı söylenebilir.

Kurumda çalışma süresi (kıdem) açısından üç değişkende de anlamlı farklılık bulunmuştur. Tekno-stres düzeyinin özellikle 11–20 yıl ve 21 yıl ve üzeri kıdeme sahip çalışanlarda daha yüksek olduğu görülmektedir. Bireysel siber güvenlik açısından 1 yıldan az ve 11–20 yıl kıdeme sahip çalışanların, özellikle 1–5 yıl kıdeme sahip çalışanlara göre daha yüksek ortalamalara sahip olduğu belirlenmiştir. Proaktif kişilikte ise 1 yıldan az kıdeme sahip çalışanların 11–20 yıl kıdeme sahip çalışanlara göre daha yüksek puan aldığı görülmektedir. Bu bulgular, kurumda çalışma süresinin özellikle tekno-stres üzerinde farklılık oluşturduğunu düşündürmektedir.

Bu bulgular birlikte değerlendirildiğinde, demografik değişkenlerin proaktif kişilik, bireysel siber güvenlik ve tekno-stres üzerinde kısmi farklılıklar oluşturduğu söylenebilir. Cinsiyet ve medeni durum bazı değişkenlerde farklılık yaratırken, statü, eğitim düzeyi ve kıdem daha belirgin farklılaşmalar ortaya koymuştur. Yaş değişkeni ise yalnızca bireysel siber güvenlik açısından anlamlı bir farklılık göstermiştir. Bu doğrultuda "H_3: Havacılık sektörü çalışanlarının demografik özellikleri ile araştırma değişkenleri arasında anlamlı farklılıklar bulunmaktadır." hipotezi kısmen kabul edilmiştir.

5. TARTIŞMA VE SONUÇ

Bu araştırma, proaktif kişilik ve bireysel siber güvenlik davranışlarının havacılık sektörü çalışanlarının tekno-stres düzeyleri ile ilişkisini ve yordayıcı rollerini incelemek amacıyla gerçekleştirilmiştir. Türkiye'de havacılık sektöründe görev yapan 387 çalışandan elde edilen veriler; korelasyon analizi, grup karşılaştırma testleri ve çoklu doğrusal regresyon analizi aracılığıyla değerlendirilmiştir. Demografik değişkenlere ilişkin karşılaştırmalarda varsayım kontrolleri dikkate alınmış; uygun durumlarda ANOVA ve Tukey HSD, varyans homojenliğinin sağlanmadığı durumlarda Welch ve Games-Howell testleri, yaş değişkeninde ise Kruskal–Wallis testi kullanılmıştır.

Çoklu doğrusal regresyon analizi sonuçları, proaktif kişilik ve bireysel siber güvenlik değişkenlerinin birlikte tekno-stres üzerinde anlamlı yordayıcılar olduğunu göstermektedir. Kurulan modelin istatistiksel olarak anlamlı olduğu belirlenmiş; proaktif kişilik ve bireysel siber güvenlik değişkenlerinin tekno-stres düzeyindeki toplam varyansın %30,8'ini açıkladığı görülmüştür. Bu oran, modelin tekno-stresi açıklamada dikkate değer (orta düzey) bir açıklayıcılığa sahip olduğuna işaret etmektedir.

Regresyon bulgularına göre, proaktif kişiliğin tekno-stres ile negatif yönlü ve anlamlı ilişkiler sergilediği yanı sıra tekno-stresin anlamlı yordayıcısı olduğu belirlenmiştir. Bu durum, proaktif bireylerin teknolojiye uyum sağlama, sorunları öngörme ve çözüm geliştirme eğilimleriyle ilişkili olabilir. Bu yönüyle proaktif kişilik, teknoloji yoğun çalışma ortamlarında tekno-stres ile ters yönlü ilişkili bir özellik olarak değerlendirilebilir. Bu bulgu, proaktif kişilik düzeyi yüksek çalışanların teknoloji kaynaklı stres düzeylerinin daha düşük olabileceğini göstermektedir. Proaktif bireylerin değişime daha açık olmaları, sorunları önceden fark edebilmeleri ve çözüm odaklı hareket etmeleri, teknoloji yoğun çalışma ortamlarında stresle daha etkili başa çıkmalarını sağlayabilir. Bu nedenle proaktif kişilik, havacılık sektörü gibi teknolojik sistemlerin yoğun kullanıldığı sektörlerde koruyucu bir bireysel özellik olarak değerlendirilebilir.

Bireysel siber güvenlik davranışlarının ise tekno-stres ile pozitif yönlü ve anlamlı ilişkiler sergilediği yanı sıra tekno-stresin anlamlı yordayıcısı olduğu belirlenmiştir. Bu bulgu, siber güvenlik farkındalığının artmasının bireylerin dijital risklere yönelik duyarlılığını ve dikkat düzeyini artırabileceğine işaret etmektedir. Bu sonuç ilk bakışta beklenenin tersine görünebilir; çünkü siber güvenlik davranışlarının çalışanı koruyucu bir rol üstlenmesi beklenebilir. Aslında bulgu, siber güvenlik farkındalığı arttıkça bireyin dijital riskleri daha fazla algıladığını, güvenlik prosedürlerine daha fazla dikkat gösterdiğini ve bu durumun teknolojiye bağlı stres deneyimini artırabileceğini düşündürmektedir. Özellikle güvenlik prosedürlerine uyum, sürekli dikkat gereksinimi ve risk algısı, teknoloji kullanım sürecinde algılanan stres düzeyiyle ilişkili olabilir. Havacılık sektörü gibi güvenlik hassasiyeti yüksek alanlarda bu sonuç daha anlaşılır hâle gelmektedir. Çalışan, yalnızca teknolojiyi kullanmakla kalmamakta; aynı zamanda dijital riskleri izlemek, prosedürlere uymak ve hata yapmama baskısını da taşımaktadır.

Standartlaştırılmış beta katsayıları birlikte değerlendirildiğinde, bireysel siber güvenliğin tekno-stres üzerindeki göreli yordayıcı gücünün proaktif kişiliğe kıyasla daha yüksek olduğu görülmektedir. Bu bulgu, tekno-stresin yalnızca bireysel uyum ve başa çıkma becerileriyle açıklanamayacağını; dijital güvenlik sorumlulukları, risk algısı ve prosedürel dikkat yüküyle de ilişkili olduğunu göstermektedir.

Bu yönüyle çalışma, tekno-stres literatürüne bireysel siber güvenlik davranışını anlamlı bir açıklayıcı değişken olarak dâhil etmesi bakımından katkı sunmaktadır.

Demografik değişkenlere ilişkin bulgular, çalışanların proaktif kişilik, bireysel siber güvenlik ve tekno-stres düzeylerinin bazı özelliklere göre farklılaştığını göstermektedir. Cinsiyet değişkeni yalnızca proaktif kişilik düzeyinde anlamlı farklılık oluşturmuş; kadın çalışanların proaktif kişilik ortalamasının erkek çalışanlara göre daha yüksek olduğu belirlenmiştir. Medeni durum açısından ise bekâr çalışanların proaktif kişilik ve bireysel siber güvenlik düzeylerinin evli çalışanlara göre daha yüksek olduğu görülmüştür. Buna karşılık, tekno-stres düzeyi cinsiyet ve medeni duruma göre anlamlı biçimde farklılaşmamıştır.

Statü değişkenine ilişkin bulgular, proaktif kişilik, bireysel siber güvenlik ve tekno-stres düzeylerinin görev türüne göre anlamlı biçimde farklılaştığını göstermektedir. Özellikle uçuş mürettebatının tekno-stres ve bireysel siber güvenlik düzeylerinin diğer gruplara kıyasla daha yüksek olması dikkat çekicidir. Bu durum, uçuş mürettebatının dijital sistemlerle yoğun etkileşim içinde bulunması, operasyonel sorumluluklarının yüksek olması ve güvenlik prosedürlerine daha doğrudan maruz kalmasıyla açıklanabilir. Proaktif kişilik açısından da uçuş mürettebatının pilotlara göre daha yüksek düzeyde olduğu belirlenmiştir. Bu bulgu, görev türünün yalnızca iş yükü ve teknoloji kullanımıyla değil, çalışanların bireysel davranış eğilimleriyle de ilişkili olabileceğini düşündürmektedir.

Yaş değişkenine ilişkin Kruskal–Wallis testi sonuçları, tekno-stres ve proaktif kişilik düzeylerinin yaş gruplarına göre anlamlı biçimde farklılaşmadığını göstermektedir. Buna karşılık bireysel siber güvenlik düzeylerinde yaş grupları arasında anlamlı farklılık tespit edilmiştir. Sıra ortalamaları incelendiğinde, 18–23 yaş grubunun bireysel siber güvenlik düzeyinin diğer yaş gruplarına göre daha yüksek olduğu görülmektedir. Bu bulgu, genç çalışanların dijital teknolojilerle daha yoğun etkileşim içinde olmaları ve siber güvenlik davranışlarına daha aşina bulunmalarıyla ilişkili olabilir.

Eğitim düzeyine ilişkin analiz sonuçları, tekno-stres ve proaktif kişilik değişkenlerinde anlamlı farklılıklar olduğunu, bireysel siber güvenlik değişkeninde ise anlamlı bir farklılık bulunmadığını göstermektedir. Tekno-stres düzeyinin özellikle lisansüstü mezunlarında ön lisans ve lisans mezunlarına göre daha yüksek olması, bu grubun daha karmaşık görevler, daha fazla sorumluluk veya daha yoğun dijital iş yüküyle karşılaşmasıyla ilişkili olabilir. Proaktif kişilik açısından ise ön lisans mezunlarının diğer eğitim gruplarına göre daha yüksek ortalamaya sahip olduğu belirlenmiştir. Bu sonuç, eğitim düzeyi ile proaktif davranış arasındaki ilişkinin doğrusal ve tek yönlü biçimde yorumlanmaması gerektiğini göstermektedir.

Kurumda çalışma süresine ilişkin bulgular, proaktif kişilik, bireysel siber güvenlik ve tekno-stres düzeylerinin kıdem gruplarına göre anlamlı biçimde farklılaştığını göstermektedir. Tekno-stres düzeyinin özellikle 11–20 yıl ve 21 yıl ve üzeri kıdeme sahip çalışanlarda daha yüksek olması, uzun süreli çalışanların değişen dijital sistemlere uyum sürecinde daha fazla zorlanabileceklerini düşündürmektedir. Bu durum, iş alışkanlıklarının yerleşmiş olması ve yeni teknolojik uygulamalara uyum ihtiyacının daha belirgin hissedilmesiyle açıklanabilir. Proaktif kişilikte ise 1 yıldan az kıdeme sahip çalışanların 11–20 yıl kıdeme sahip çalışanlara göre daha yüksek puan alması, kuruma yeni katılan bireylerin uyum sağlama, kendini gösterme ve sorumluluk alma eğilimlerinin daha belirgin olabileceğine işaret etmektedir.

Araştırma bulguları genel olarak değerlendirildiğinde, havacılık sektöründe tekno-stresin hem bireysel kişilik özellikleri hem de dijital güvenlik davranışlarıyla ilişkili olduğu görülmektedir. Proaktif kişilik ile tekno-stres arasında ters yönlü bir ilişki bulunurken, bireysel siber güvenlik davranışları ile tekno-stres arasında aynı yönlü bir ilişki belirlenmiştir. Bu nedenle örgütlerin dijital güvenlik eğitimlerini yalnızca teknik bilgi aktarımı olarak değil, aynı zamanda stres yönetimi ve psikolojik dayanıklılık boyutuyla birlikte ele almaları önem taşımaktadır. Siber güvenlik farkındalığı artırılırken, çalışanların bu farkındalığı sürekli bir tehdit algısına dönüştürmemesi için destekleyici uygulamalar geliştirilmelidir.

Elde edilen bulgular literatürle büyük ölçüde örtüşmektedir. Proaktif kişilik ile stres düzeyi arasındaki negatif ilişki, Bateman ve Crant (1993) ile Seibert, Crant ve Kraimer (1999) tarafından ortaya konulan proaktif davranış kuramı çerçevesiyle uyumludur. Proaktif bireylerin çevresel talepleri pasif biçimde kabullenmek yerine dönüştürmeye çalışmaları, teknoloji kaynaklı stres faktörlerinin etkisini azaltabilmektedir.

Bununla birlikte, siber güvenlik davranışı ile tekno-stres arasındaki pozitif ilişki literatürde görece daha az tartışılmış bir bulgudur. Mevcut çalışmalar genellikle siber güvenlik davranışının örgütsel güvenlik performansı üzerindeki olumlu etkilerine odaklanırken, bu araştırma artan farkındalığın bireyde risk algısını ve sorumluluk baskısını artırarak stres düzeyini yükseltebileceğini göstermektedir (Hadlington, 2017; Parsons, McCormac, Butavicius, Pattinson ve Jerram, 2014). Bu durum, "koruyucu bilinç – psikolojik yük" paradoksu çerçevesinde değerlendirilebilir. Dolayısıyla çalışma, siber güvenlik düzeyinin yalnızca teknik bir yetkinlik değil, aynı zamanda psikolojik bir yük unsuru olabileceğini ortaya koyarak literatüre özgün bir katkı sunmaktadır.

Araştırmanın bazı sınırlılıkları bulunmaktadır. Öncelikle örneklem yalnızca havacılık sektöründe çalışan bireylerle sınırlıdır; bu nedenle bulguların farklı sektörlere genellenmesi dikkatle yapılmalıdır. Verilerin kesitsel yapıda olması nedensellik çıkarımlarını sınırlamaktadır. Ayrıca öz-bildirim yoluyla toplanan veriler sosyal istenilirlik yanlılığı riskini içermektedir. Modelde yalnızca iki bağımsız değişkenin yer alması da tekno-stresin çok boyutlu yapısının tümüyle açıklanmasına imkân vermemektedir.

Gelecek araştırmalarda farklı sektörlerde ve kültürel bağlamlarda benzer modellerin test edilmesi önerilmektedir. Yanı sıra boylamsal çalışmalar ile değişkenler arasındaki nedensel ilişkiler daha güçlü biçimde incelenebilir. Psikolojik dayanıklılık, dijital okuryazarlık, iş yükü, örgütsel destek ve teknolojiye yönelik tutum gibi aracı veya düzenleyici değişkenlerin modele eklenmesi, tekno-stresin daha kapsamlı biçimde anlaşılmasına katkı sağlayabilir.

Uygulayıcılar açısından değerlendirildiğinde, siber güvenlik eğitimlerinin stres yönetimi boyutuyla birlikte ele alınması ve proaktif davranışları destekleyen örgütsel uygulamaların geliştirilmesi önerilmektedir. Havacılık sektörü gibi teknoloji yoğun sektörlerde çalışan personel için kullanıcı dostu sistem tasarımları ve teknik destek mekanizmaları güçlendirilmelidir. Proaktif kişilik özelliklerini destekleyen örgütsel kültür ve eğitim programları, çalışanların teknolojik değişime uyum kapasitesini ve teknolojik stresle başa çıkma becerilerini artırabilir. Kurumların yalnızca teknik yetkinliklere değil, bilişsel esneklik ve davranışsal uyum becerilerine de yatırım yapması önem taşımaktadır.

Bu çalışma, bireysel siber güvenlik davranışının tekno-stres üzerinde pozitif ve anlamlı bir yordayıcı rol üstlendiğini ortaya koyarak ilişkinin yönüne dair dikkat çekici bulgular sunmuştur. Proaktif kişilik ile tekno-stres arasındaki negatif ilişki ise, bireylerin değişime uyum sağlama ve problem çözme eğilimlerinin teknoloji kaynaklı stres deneyimini azaltabileceğine işaret etmektedir. Havacılık sektörü bağlamında elde edilen bu bulgular, tekno-stresin yalnızca bireysel özelliklerle değil, dijital güvenlik sorumlulukları, görev türü, eğitim düzeyi ve kıdem gibi yapısal ve örgütsel faktörlerle birlikte değerlendirilmesi gerektiğini göstermektedir. Ayrıca demografik değişkenlere ilişkin karşılaştırma analizleri, çalışan grupları arasında farklılaşan teknoloji ve güvenlik deneyimlerinin örgütsel politika ve destek mekanizmaları açısından dikkate alınması gerektiğini ortaya koymaktadır.

Kaynaklar

Akın, A., Abacı, R., Kaya, M. ve Arıcı, N. (2011). *Kısaltılmış Proaktif Kişilik Ölçeği'nin (KPÖ) Türkçe formunun geçerlik ve güvenirliği*. Paper presented at the ICES11 International Conference on Educational Sciences, June, 22-25, Famagusta, Cyprus.

Altıntaş, M. ve Altıntaş, B. (2026). Aile ve Denge: Havayolu Kabin Memurlarında İş Yaşam Dengesi, Teknostres ve Kariyer Stresi İlişkisi. *Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 12*(Aile Özel Sayısı), 318-337.

Altıntaş, M., Şanlı, A. ve Odacı, D. (2026). Havalimanı Yer Hizmetlerinde Teknostres: Bilinçli Farkındalık Etkisinde Psikolojik Dayanıklılığın Aracı Rolü, *Üçüncü Sektör Sosyal Ekonomi Dergisi, 61*(1), 766-789.

Antonacopoulou, E. P. (2000). Employee Development Through Self-Development in Three Retail Banks. *Personnel Review, 29*(4), 491-508.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: technological antecedents and implications. *MIS Quarterly, 35*(4), 831–858.

Bateman, T. S., & Crant, J. M. (1993). The proactive component of organizational behavior: A measure and correlates. *Journal of Organizational Behavior, 14*, 103-118.

Bateman, T. S., & Crant, J. M. (1999). Proactive Behavior: Meaning, Impact, Recommendaions. *Business Horizons, 42*(3), 63-70.

Bolino, M. C., Valcea, S., & Harvey, J. (2010). Employee, Manage Thyself: The Potentiallynegative Implications of Expecting Employees to Behave Proactively. *Journal of Occupational and Organizational Psychology, 83*(2), 325-345.

Brod, C. (1984). *Technostress: The Human Cost of the Computer Revolution*. Reading, MA: Addison-Wesley.

Büyüköztürk, Ş. (2007). Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı, *Eğitim Yönetimi Dergisi. Güz*, *32*, 470-483.

Cadieux, N., Cadieux, J., Youssef, N., & Mosconi, E. (2020). Techno(Stress) and Techno(Distress): Validation of a specific techno-stressors index among Quebec lawyers. *Behaviour & Information Technology, 39*, 1079–1093.

Caprara, G. V., & Cervone, D. (2003). *A Conception of Personality For A Psychology of Human Strengths: Personality as An Agentic, Self-Regulating System.* L. G. Aspinwall & U. M. Staudinger (Ed.), A Psychology of Human Strengths: Fundamental Questions and Future Directions For A Positive Psychology. Washington: American Psychological Association.

Claes, R., Beheydt, C., & Lemmens, B. (2005). Unidimensionality of abbreviated proactive personality scales across cultures. *Applied Psychology*, *54*(4), 476-489.

Crant, J. M. (1995). The Proactive Personality Scale and Objective Job Performance Among Real Estate Agents. *Journal of Applied Psychology, 80*(4), 532-537.

Crant, J. M., & Bateman, T. S. (2000). Charismatic Leadership Viewed From Above: The Impact of Proactive Personality. *Journal of Organizational Behavior, 21*(1), 63-75.

Covey, S. (2010). *Etkili İnsanların 7 Alışkanlığı* (37 b.). (O. Deniztekin ve F. N. Deniztekin, Çev.) İstanbul: Varlık Yayınları.

Çelik, E. ve Kara, S. (2017). Heyecan Arayışının Yaşam Doyumu ile Proaktif Kişilik Arasındaki İlişkide Baskıcı Etkisi. *Mediterranean Journal of Humanitie, 7*(1), 123-134.

Çoban, R. ve Bükeç, C. M. (2021). Proaktif kişilik özelliğinin bilgi ifşasına etkisi: hava trafik kontrolörleri üzerine bir araştırma. *Journal of Aviation, 5*(2), 150-169.

Çubukçu, A. ve Bayram Ş. (2013). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research, 5*, 148-174.

De Moor, S., Dock, M., Gallez, S., Lenaerts, S., Scholler, C., & Vleugels, C., (2008). Teens and ICT: Risksand Opportunities. 11.10.2025 tarihinde http://www.belspo.be/ belspo/fedra/TA/synTA08_nl.pdf.

Erol, O., Şahin, Y. L., Yılmaz, E. ve Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences, 12*(2), 75-91.

Frankl, V. E. (1994). *Duyulmayan Anlam Çığlığı.* (S. Budak, Çev.) 2.Baskı, Ankara: Öteki Yayınevi.

Fuller, B., & Marler, L. E. (2009). Change Driven by Nature: A Meta-Analytic Review of the Proactive Personality Literature. *Journal of Vocational Behavior, 75*, 329-345.

Garfinkel, S. L. (2012). The cybersecurity risk. *Magazine Communications of the ACM, 55*(6), 29-32.

Gence, Z., Ural, S. A. ve Aksu, E. (2024). İş tatmini ve işten ayrılma niyeti arasındaki ilişkide iş yükü ve proaktif kişiliğin düzenleyici rolü: Havacılık sektöründe bir araştırma modeli. *Human Factors in Aviation and Aerospace, 1*(1), 56-70.

Graham, J., & Howard, R. (2010). *Cyber Security Essentials.* Boca Raton: Auerbach Publications.

Gupta, V. K., & Bhawe, N. M. (2007). The Influence of Proactive Personality and Stereotype Threat on Women's Entrepreneurial Intentions. *Journal of Leadership and Organizational Studies, 13*(4), 73-85.

Gürbüz, S. ve Şahin, F. (2014) *Sosyal Bilimlerde Araştırma Yöntemleri*, 1.Baskı, Ankara: Seçkin Yayıncılık.

Güriş, S. ve Çağlayan, E. (2005). *Ekonometri (2. Basım),* İstanbul: Der Yayınları.

Hadlington, L. (2017). Human factors in cybersecurity; Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346.

Ilgaz, G., Özgür, H. ve Çuhadar, C. (2016). The Adaptation of Technostress Scale into Turkish. *Abstracts of the 11th International Balkan Education and Science Congress*, (p.69), Poreč, Croatia.

Kalaycı, Ş. (2010). *SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri*, *5.Baskı*, Ankara: Asil Yayın Dağıtım.

Kalaycı, Ş. (2014). *SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri*, 6.*Baskı*, Ankara: Asil Yayıncılık.

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, 675-705.

Lazarus, R., & Folkman, S. (1984). *Stress, Appraisal, and Coping.* New York: Springer.

Lee, S. M., & Peterson, S. (2000). Culture, Entrepreneurial Orientation and Global Competitiveness. *Journal of World Business, 35*(4), 401-416.

Norhisham, N. (2021). Understanding Technostress During the Era of Covid-19: A Conceptual Paper. *International Journal of Academic Research in Business and Social Sciences, 11*(8), 1936–1947.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

Ragu-Nathan, T., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research, 19*(4), 417- 433.

Salanova, M., Llorens, S., & Cifre, E. (2013). The dark side of technologies: Technostress among users of information and communication technologies. *International Journal of Psychology, 48*(3), 422-436.

Seibert, S. E., Crant, J. M., & Kraimer, M. L. (1999). Proactive personality and career success. *Journal of Applied Psychology, 84*(3), 416–427.

Seibert, S. E., Kraimer, M. L., & Crant, J. M. (2001). What Do Proactive People Do? A Longitudinal Model Linking Proactive Personality and Career Success. *Personnel Psychology, 54*(4), 845-874.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying, its forms and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49,* 376–385.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The Impact of Technostress on Role Stress and Productivity. *Journal of Management Information Systems*, *24*(1), 301–328.

Tarafdar, M., Tu, Q., & Ragu-Nathan, T. S. (2011). Impact of Technostress on End-User Satisfaction and Performance. *Journal of Management Information Systems*, *27*, 303-334.

Thompson, J. A. (2005). Proactive Personality and Job Performance: A Social Capital Perspective. *Journal of Applied Psychology, 90*(5), 1011-1017.

Uncuoğlu Yolcu, İ. ve Çakmak, A. F. (2017). Proaktif Kişilik İle Proaktif Çalışma Davranışı İlişkisi Üzerinde Psikolojik Güçlendirmenin Etkisi. *Uluslararası Yönetim İktisat ve İşletme Dergisi, 13*(2), 425-438.

Valcke, M., Bonte, S., De Wever, B., & Rots, I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers & Education, 55*(2), 454-464.

Verešová, M., & Malá, D. (2012). Stress, proactive coping and self-efficacy of teachers. *Procedia-Social and Behavioral Sciences, 55*, 294-300.

Yeşil, M. (2022). *Lise Öğrencilerinin Kariyer Kararsızlıkları ve Proaktif Kişilik Özellikleri Arasındaki İlişkide Azmin Aracı Rolü*. Doktora Tezi. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü: Adana.

Research Article

Proaktif Kişilik ve Bireysel Siber Güvenliğin Tekno-Stres Üzerindeki Etkisi: Havacılık Sektörü Çalışanlarına Yönelik Bir Araştırma

The Impact of Proactive Personality and Individual Cybersecurity on Technostress: A Study on Aviation Sector Employees

Ahmet DENİZ

Dr. Öğr. Üyesi, İstanbul Gelişim Üniversitesi

Uygulamalı Bilimler Fakültesi

ahdeniz@gelisim.edu.tr

https://orcid.org/0000-0002-3878-6331

Extended Summary

The rapid digital transformation of contemporary workplaces has fundamentally reshaped organizational processes, job structures, and employee roles. The increasing integration of information and communication technologies into daily work practices has significantly improved efficiency and productivity, while simultaneously introducing new psychological demands and challenges for employees. One of the most prominent outcomes of this transformation is technostress, which refers to the stress individuals experience due to difficulties in adapting to and coping with technological requirements. In high-reliability and technology-intensive sectors such as aviation, where digital systems are deeply embedded in operational, safety-critical, and decision-making processes, understanding the factors associated with technostress is of particular importance. In such environments, employee stress not only affects individual well-being but may also influence organizational performance, operational safety, and decision-making quality.

Although prior research has largely focused on organizational and technological determinants of technostress—such as system complexity, workload, and organizational support—individual-level psychological and behavioral variables have received comparatively less attention. In this context, the present study aims to examine the relationships and predictive roles of proactive personality and individual cybersecurity behaviors in relation to technostress among aviation sector employees in Türkiye. By integrating these variables into a single analytical framework, the study seeks to provide a more comprehensive understanding of technostress in digitally intensive work environments.

The study is grounded in Lazarus and Folkman's Cognitive Appraisal Theory, which conceptualizes stress as a result of individuals' evaluations of environmental demands. According to this theory, individuals interpret external stimuli as either threatening or manageable, and this cognitive appraisal process shapes their emotional and behavioral responses. Within this framework, proactive personality and individual cybersecurity behaviors are conceptualized as cognitive–behavioral factors associated with how employees perceive and respond to digital stressors. Proactive individuals tend to take initiative, anticipate potential problems, and actively shape their environment, whereas cybersecurity behaviors reflect individuals' awareness and actions regarding digital safety, risk management, and compliance with security procedures.

The study employed a quantitative research design based on a relational survey model. Data were collected from 387 employees working in public and private aviation organizations in Türkiye, including pilots, flight crew members, and ground support personnel. Participation was voluntary, and ethical

approval was obtained prior to data collection. The data collection instrument consisted of four sections: demographic variables and three validated scales measuring proactive personality (α = .813), technostress (α = .874), and individual cybersecurity behaviors (α = .787). All measurement tools demonstrated acceptable to high levels of internal consistency reliability. The data were analyzed using SPSS 26, and the analysis included descriptive statistics, Pearson correlation analysis, independent samples t-tests, group comparison tests (ANOVA, Welch, Games-Howell, and Kruskal–Wallis), and multiple linear regression analysis.

The findings revealed statistically significant relationships among the main variables. Proactive personality was positively and weakly correlated with individual cybersecurity behaviors ($r = .19$, $p < .01$). In addition, proactive personality was negatively and significantly associated with technostress ($r = -.16$, $p < .01$), indicating that higher levels of proactivity are related to lower levels of technology-induced stress. In contrast, individual cybersecurity behaviors were positively and moderately associated with technostress ($r = .49$, $p < .001$), suggesting that increased cybersecurity awareness and behaviors are related to higher levels of technostress.

To further examine the predictive roles of the independent variables, a multiple linear regression analysis was conducted. The results indicated that the overall model was statistically significant ($F(2,384) = 85.529$, $p < .001$), with a moderate level of explanatory power ($R^2 = .308$; Adjusted $R^2 = .305$). This finding suggests that proactive personality and individual cybersecurity behaviors together explain approximately 30.8% of the variance in technostress.

When the regression coefficients were examined, proactive personality was found to be a negative and significant predictor of technostress ($\beta = -.265$, $p < .001$), supporting H1. This result indicates that employees with higher levels of proactive personality tend to experience lower levels of technostress. This finding can be explained by the tendency of proactive individuals to adapt more quickly to technological changes, anticipate potential problems, and develop effective coping strategies.

On the other hand, individual cybersecurity behaviors were found to be a positive and significant predictor of technostress ($\beta = .541$, $p < .001$), supporting H2. This result suggests that employees who exhibit higher levels of cybersecurity awareness and engagement tend to report higher levels of technostress. Moreover, standardized beta coefficients indicate that cybersecurity behaviors have a stronger predictive effect on technostress compared to proactive personality. This finding highlights that cybersecurity-related responsibilities may increase cognitive load, perceived risk, and procedural pressure, thereby contributing to higher stress levels.

The positive association between cybersecurity behaviors and technostress may be interpreted through the lens of increased risk awareness and vigilance. Employees who are more knowledgeable about digital threats and security protocols may become more sensitive to potential risks, leading to heightened attention and perceived responsibility. This situation may create a paradox in which behaviors that are beneficial for organizational security may simultaneously increase psychological burden. However, given the cross-sectional nature of the data, these interpretations should be considered as associative rather than causal.

Analyses based on demographic variables revealed partial differences across the study constructs, supporting H3 partially. Gender differences were observed only in proactive personality, with female employees reporting higher levels than males. No significant gender differences were found in technostress or cybersecurity behaviors. Marital status was associated with differences in both proactive personality and cybersecurity behaviors, with single employees reporting higher levels than married employees, while technostress did not differ significantly.

Occupational status was found to be associated with all three variables. Flight crew members reported higher levels of technostress and cybersecurity behaviors compared to pilots and ground support personnel. Additionally, proactive personality levels were higher among flight crew compared to pilots. Age was associated only with cybersecurity behaviors, with younger employees demonstrating higher levels. Education level was associated with differences in proactive personality and technostress, while no significant differences were found in cybersecurity behaviors. Organizational tenure was found to significantly differentiate all three variables, with higher technostress levels observed among employees with longer tenure.

From a theoretical perspective, the study contributes to the technostress literature by integrating both psychological (proactive personality) and behavioral (cybersecurity behaviors) variables into a unified model. The coexistence of a negative relationship between proactive personality and technostress and a positive relationship between cybersecurity behaviors and technostress reveals a complex dynamic that may be conceptualized as a "protective awareness–psychological burden" paradox. This perspective extends existing literature by demonstrating that not all adaptive behaviors necessarily reduce stress; some may increase psychological demands.

From a practical standpoint, the findings suggest that organizations—particularly in technology-intensive sectors such as aviation—should adopt a balanced approach when promoting cybersecurity practices. While enhancing cybersecurity awareness is essential, it is equally important to consider its potential psychological implications. Integrating stress management components into cybersecurity training programs may help reduce unintended stress outcomes. Additionally, fostering proactive personality traits through organizational culture, leadership practices, and training initiatives may enhance employees' ability to cope with technological demands.

Despite its contributions, the study has certain limitations. The use of cross-sectional data limits causal interpretations, and the reliance on self-reported measures may introduce common method bias. Furthermore, the sample is limited to aviation sector employees in Türkiye, which may restrict generalizability. Future research may employ longitudinal designs and incorporate additional variables such as psychological resilience, organizational support, workload, and digital literacy to further explain technostress.

In conclusion, the study demonstrates that proactive personality functions as a mitigating factor against technostress, whereas individual cybersecurity behaviors, despite their protective nature, may increase stress levels. By integrating individual-level psychological and behavioral factors into the technostress framework, the study provides a more comprehensive understanding of technology-related stress in high-risk and technology-intensive work environments.