Uluslararası Ekonomi ve Yenilik Dergisi, 12(1) 2026, 17-32

International Journal of Economics and Innovation, 12(1) 2026, 17-32

https://doi.org/10.20979/ueyd.1756755

Türk Dünyasında Siber Güvenlik Alanında Yapılan Çalışmaların Analizi

Araştırma Makalesi /Research Article

Fatih Çağatay BAZ[1]
Elnur PAŞA[2]

ÖZ: *Teknolojide yaşanan gelişmeler, özellikle internet tabanlı teknolojiler ile siber güvenlik kavramının önemini ortaya koymaktadır. Bu çalışma ile siber güvenlik alanında Türk dünyasında gerçekleştirilen araştırmaların eğilimlerinin belirlenmesi amaçlanmıştır. Çalışma kapsamında 2008 ile 2025 (19.03.2025'e kadar) tarih aralığında yayınlanan Türk dünyası kapsamında siber güvenlik konulu çalışmaların bibliyometrik analizi Web of Science (WOS) veri tabanı ve R veri analiz programı üzerinde hazırlanarak, Biblioshiny Biblimetrix paket yazılımı kullanılarak gerçekleştirilmiştir. Bu kapsamda Türk dünyası ülkeleri Türkiye, Azerbaycan, Kazakistan, Kırgızistan ve Özbekistan ile ilgili 805 çalışmaya ulaşılarak bibliyometrik analizi yapılmıştır. Araştırmada yayın, yıllar, yazarlar, ülkeler ve araştırma alanları gibi farklı parametreler kullanılarak analiz çalışması gerçekleştirilmiştir. Elde edilen bulgular ile yıllara göre atıf sayıları, kelime bulutu, tematik harita, anahtar kelime trendleri, ülke, anahtar kelime ve başlıklara ait üç alan grafiği, ülkelere ait yoğunluk haritalarına yer verilerek siber güvenlik üzerine çeşitli sonuçlar ortaya konulmuştur. Yapılan analiz ile mevcut çalışmalarda siber güvenlik konusuna ilişkin araştırmaların kapsamlı bir değerlendirmesi sunulmuş ve gelecekte yapılması planlanan araştırmalara yol göstermesi amaçlanmıştır.*

Anahtar Kelimeler: *Bibliyometrik analiz, Siber güvenlik, Türk dünyası*

Analysis of Studies Conducted in the Field of Cyber Security in the Turkic World

ABSTRACT: *The developments in technology, especially with internet-based technologies, reveal the importance of the concept of cyber security. This study aims to determine the trends in research conducted in the Turkish world in the field of cyber security. Within the scope of the study, bibliometric analysis of studies on cyber security within the Turkish world published between 2008 and 2025 (until 19.03.2025) was prepared on the Web of Science (WOS) database and R data analysis program and was carried out using the Biblioshiny Biblimetrix package software. In this context, 805 studies related to the Turkish world countries of Türkiye, Azerbaijan, Kazakhstan, Kyrgyzstan and Uzbekistan were reached and their bibliometric analysis was performed. The analysis study was carried out using different parameters such as publication, years, authors, countries and research areas. With the findings obtained, various results on cyber security were presented by including the number of citations by year, word cloud, thematic map, keyword trends, three area graphs for countries, keywords and titles, and density maps for countries. The analysis provided a comprehensive evaluation of existing studies on cyber security and aimed to guide future research.*

Keywords: *Bibliometric analysis, Cyber security, Turkish world*

[1]Doç. Dr. Osmaniye Korkut Ata Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, fatihcagataybaz@osmaniye.edu.tr; https://orcid.org/00000-0002-6398-9851

[2]Dr. Öğr. Üyesi, Milli Savunma Üniversitesi, Kara Harp Okulu, elnurpasa@yahoo.com; https://orcid.org/00000-0001-6723-7617

Geliş Tarihi / Received: 02/08/2025

Kabul Tarihi / Accepted: 24/11/2025

1.Giriş

Teknolojide yaşanan gelişmeler ile siber güvenliğin önemi artmaktadır. Bu anlamda ülkeler gerekli önlemleri almak, ulusal ve uluslararası siber saldırılarla mücadele etmek zorundadır. Siber saldırılar, hedef alınan ülkenin sivil ve askeri yapısına zarar verebilmektedir.

Siber saldırılar, yanlış bilgi yaymak, taktiksel hizmetleri sekteye uğratmak, hassas bilgilere erişmek, casusluk yapmak, veri hırsızlığı yapmak ve maddi kayıplara yol açmak için kullanılmaktadır. Siber eylemleri önlemek ve gereken tedbirleri almak adına kapsamlı araştırmalar yapılmalı, etkili bir teknik altyapı oluşturulmalıdır (Uma ve Padmavathi, 2013). Özellikle internet kullanımının hızla yaygınlaşması siber güvenlik konusunda alınması gereken tedbirleri bireysel, kurumsal hatta devletler nezdinde zorunlu kılmaktadır.

Siber güvenlik alanında, jeopolitik olaylar ve siber saldırılar konusunda bir korelasyon olduğu ifade edilebilir. Türkiye'nin ve Türk Devletlerinin jeopolitik hadiselerinin yaşandığı dönemlerde siber hareketliliklerin o ülkeler aleyhine arttığı gözlenmektedir (Çalıkoğlu, 2024). Siber güvenliğin uluslararası alanda, politikada etki aracına dönüştüğü de yapılan çalışmalarda görülmektedir (Karataş, 2020; Gündoğdu, 2023). Siber tehditlerin artan çeşitliliği, ülkeler için siber güvenliğe olan ihtiyacı göstermektedir (Güntay, 2018; Çifci, 2024). Siber saldırıların etkisini kaybetmeden artmaya devam edeceği, farklı ülkelerde meydana geleceği ve olumsuz sonuçlar doğuracağı yüksek ihtimal dâhilindedir (Arslan, 2021). Günümüzde kullanılan elektronik cihazların kendi aralarında haberleşmeleri nesnelerin interneti (IoT), kablosuz ağlar, endüstri 4.0 gibi yazılım ve elektronik alanlardaki gelişmeler ile siber güvenlik konusunda güvenlik açıkları tespit edilerek önlemler alınması gerekmektedir (Acarer, 2020). Bu anlamda başta kritik altyapıya sahip kurum ve kuruluşların siber güvenliklerinin sağlanması devletlerin en önemli önceliklerinden birisi durumuna gelmiştir (Darıcılı, 2019). Türkiye siber güvenlik konusunda önemli aşamalar kaydetmiştir. Siber suçlarla ilgili kanunlar 1991 yılından itibaren yürürlüğe girmiştir (Deniş ve Demircioğlu, 2023). Türkiye'de siber güvenliği sağlamada; Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME), TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) bünyesinde kurularak faaliyete geçirilen bir kurumdur (Hekim ve Başıbüyük, 2013). Aksi taktirde ülkelerin savunma sistemleri de olmak üzere ekonomik, askeri ve politik sorunlar oluşacaktır.

Siber savaş tehditlerinin artması ile devletler siber saldırılar karşısında yapmaları gerekenleri araştırmakta ve yeteneklerini geliştirmektedir (Yanarışık, 2020). Tüm dünyada olduğu gibi Türk dünyasında siber güvenlik konusu önem arz etmektedir. Gürdal-Limon (2023), devletlerin kendi başlarına sorunlarla başa çıkmada, self-help olarak adlandırılmaktadır, ulusal güvenliklerinin bir parçası olan siber güvenlik konusunda tedbirler alınması gerektiğini belirtmektedir. Bunu gerçekleştirmede askeri birimler başta olmak üzere Savaş Yönetim Sistemlerine (SYS) ihtiyaç duymaktalardır. Türk dünyası devletleri siber savaş ortamında saldırı

kaynağı, saldırı türü ve saldırı yeri gibi verilere ulaşım sağlamak zorundadır. Siber saldırılar üzerinden gerçekleştirilen terörizm faaliyetleri sebebiyle, devletlerin siber konular üzerine ortak anlaşmalar imzalamaları kaçınılmaz olmuştur (Güneş, 2019). Bu anlamda Türkiye ve Azerbaycan arasında imzalanan Şuşa Beyannamesi ile siber güvenlik ve medya alanında da iş birliği yapılması kararlaştırılmıştır (Özdemir ve Kantar, 2023).

Teknolojik gelişmelerin yol açtığı dönüşüm sayesinde küresel anlamda askerî savaşlar siber savaşlara evrilmiştir. Bundan kaynaklı savunma harcamaları da yeni harcama kalemleri ortaya çıkarmıştır (Efe ve Afşar, 2023). Son yıllarda Türkiye'nin yakın çevresinde bulunan ülkelerden Estonya, Ukrayna, İran'a da ülkelerarası siber saldırılar yapılmış ve bu ülkelerdeki farklı sistemlere ve ekonomilerine ciddi zararlar verilmiştir (Acarer, 2020). Yapılan siber saldırılar bilişim altyapılarını bozmakta, kesintiye uğratmakta veya aksamalara sebep olmaktadır (Dilek ve ark., 2023). Özellikle enerji sektöründe yer alan aktör ülkeler açısından, siber savaş ve siber terör kritik düzeyde tehdit unsuru oluşturmaktadır (Aydın ve ark., 2021). Siber savaş, bilgi savaşı kavramı içerisinde yer almakta ve ülkelerin siber ortamda gerçekleştirdikleri mücadeleyi ifade etmektedir (Yayla, 2013). Siber terör ise, siyasi veya sosyal alanlara baskı kurmak veya zarar vermek amacıyla, ilgililerin bilgisayarlarına, ağ sistemlerine istemli olarak yapılan geniş kapsamlı eylemlerdir (Yılmaz, 2020). Hatta yeni bir kavram olarak yer edinen karma savaş; konvansiyonel tehdit ve şantajın yanı sıra siber saldırının da yer aldığı bir tehdit olarak belirtilen bir savaş türüdür (Erol ve Oğuz, 2018). Türkiye'nin ve Türk Dünyası ülkelerinin bölgesel siber savunmada, milli yazılım ve donanım geliştirmelerinde birlikte hareket etmeleri gerekmektedir. Bu sayede stratejik olarak siber tehditlerin azaltılması ve dayanıklılığın sağlanmasında kolektif çalışmalar etkili olacaktır (Özdemir, 2025).

Siber güvenlik konusu farklı disiplinleri, sektörleri, aktörleri ve bileşenleri bulundurmakta, tüm bu değişkenleri bir araya getirecek bir yönetişim modeli başarılı olabilecektir. Resmi-gayri resmi, devlet-özel ayrımı olmaksızın ekonomik, sosyal, siyasal, teknik, kültürel ve hukuksal boyutları bulunan siber güvenlik sorunu yine bütün bu bileşenlerle beraber ele alındığında çözülecektir (Kutlu ve ark., 2019). Bu gerekçelerden ötürü siber güvenlik alanında Türkiye ve Türk Devletlerinin birlikte hareket etmesi zorunludur.

2. Literatür Taraması

Literatür incelendiğinde siber güvenlik konusunda birçok çalışmanın bulunduğu görülmektedir. Güntay (2018), çalışmasında siber güvenliğin uluslararası politika alanında nasıl etki aracına dönüştüğünü ve uluslararası aktörleri ortaya koymaktadır. Çalışmada siber saldırılar, siber istihbarat uluslararası politikalar çerçevesinde ele alınmıştır. Ayrıca çalışmada aktörler ile ilgili değerlendirmelerin yanı sıra teorik ve pratik ögeler de analiz edilmiştir. Araştırma sonuçlarına göre siber güvenlik alanında farklı türden teorik yaklaşımların uluslararası ilişkiler boyutunda tutarsızlaşmaya başladığı, siber güvenlik saldırılarının ve savunma

yöntemlerinin eksiksiz ve net şekilde ortaya konulamayışından kaynaklandığı belirtilmiştir.

Acarer (2020) ülke güvenliğinde alınabilecek makro siber güvenlik önlemleri konusunda çalışma yapmıştır. Bu çalışmada siber güvenlik konusunda Türkiye'de politika ve stratejilerin yeniden gözden geçirilmesi gerektiğini ortaya koymuştur. Bu konuda alınabilecek önlemlerin acilen ortaya konulmasının ve uluslararası hukuki bir çerçeveye alınmasının zorunluluk oluşturduğunu ifade etmektedir. Ayrıca çalışmada siber güvenlik alanında çözüm önerileri ve uygulama örnekleri de ortaya konulmuştur.

Aydın ve diğerleri (2021) tarafından betimleme yöntemiyle yapılan araştırmada enerji sistemlerinde siber güvenlik kavramlarının genel çerçevesini çizme amaçlanmıştır. Bu anlamda enerji alanında yaşanan siber saldırılar araştırılmış, SCADA ile yönetilen, özellikle enerji sistemleri altyapılarında mevcut farkındalığın sağlanmasına yönelik öneriler sunulmuştur. Araştırma sonuçlarına göre siber güvenlik konusunda enerji sistemleri alanının hayati öneme sahip olduğu ifade edilmektedir. Ayrıca Türkiye'de yerli şirketler tarafından tasarlanan ve test edilen milli siber güvenlik sistemleri ve ürünlerinin enerji sektöründe kullanılması konusunda ayrıca vurgu yapılmıştır.

Çakır ve Taşer (2023) çalışmalarında Türkiye'de yapılan siber güvenlik alanındaki faaliyetlerin ve eğitim çalışmalarının değerlendirmesini gerçekleştirmişlerdir. Çalışmada siber güvenlik alanında Türkiye'de son yirmi yılda yapılan çalışmalara ait strateji ve politikalar incelenerek olumlu ve olumsuz yönler ortaya konulmaya çalışılmıştır. Araştırma bulgularına göre siber güvenlik alanında bilişim suçlarına ilişkin mevzuat henüz incelenmemiştir. 2000'li yıllarda daha yetersiz olan siber güvenlik önlemlerine rağmen, 2012 itibariyle ciddi önlemler alınmaya başlanmıştır. Araştırma sonuçlarında akademik çalışmalardaki artış, yerli – milli yazılım ve donanımlardaki gelişmelerin Türkiye'nin önümüzdeki süreçte ilerlemeye kaydedeceği şeklinde belirtilmiştir.

Ulusal Siber Olaylara Müdahale Merkezi (USOM)'nin uluslararası politikada etkin bir araç olarak Türkiye'nin siber güvenlik alanındaki uygulaması ile ilgili Gündoğdu (2023) bazı sorunların ve çözüm yollarının ortaya konulması çalışmasını gerçekleştirmiştir. Çalışmada Türkiye'nin siber uzayda kamu hizmetleri açısından durumu, siber güvenlik alanında planladığı politikalar, ülke olarak strateji ve eylem planının neler olduğu ortaya konulmuştur. USOM başta olmak üzere, kurumların etki aracı olmaları da araştırma sonuçlarında ortaya konulmuştur.

Gürdal-Limon (2023) çalışmasında, siber güvenlik konusunda ulusal düzeyde güvenlik payı büyüdüğünde devletlerin kendi başlarına hareket etme eğilimlerinin arttığını vurgulamaktadır. Çalışmada siber güvenlik konusu uluslararası ilişkilerde bir güç unsuru olarak ele alınmakta, askeri teçhizatların yerli ve milli olma konusunda analiz edilmekte, yapısalcı yaklaşım ile yeniliklerin yeri belirlenmeye çalışılmaktadır. Bu anlamda Türk menşeili savunma şirketleri ile Savaş Yönetim

Sistemleri çalışmanın inceleme alanıdır. Çalışmada uluslararası düzeyde enstitü indeksleri ve siber veri indeksleri aracılığı ile siber güvenlik endişeleri de ortaya konulmuştur.

Çalıkoğlu (2024) çalışmasında kolektif siber güvenliğin önemi ve Türk Devletler Teşkilatı bünyesinde yapılması gerekenlere yer vermiştir. Siber güvenlik ve siber saldırılar, son yıllarda gerçekleşen dünya genelindeki siber saldırılar, ülkeler arası siber güvenlik yapıları hakkında çalışmada detaylı bilgiler verilmiştir. Çalışma Türk Devletleri Teşkilatı çatısı altında yer alan ülkelerin kolektif siber savunma gücü oluşturması adına önerilerde bulunmuştur.

Türkiye'nin siber güvenlik olgunluğunu NCAF çerçevesinde değerlendiren Çifci (2024), kurum kuruluşlar başta olmak üzere kapsamlı bir literatür taraması ile durumu ortaya koymuştur. Yapılan çalışmada, NCAF değerlendirmesi ile Türkiye'nin yüksek siber güvenlik seviyesinde olduğu ancak tedarik zinciri, acil durum stratejisi, eğitim-öğretim ve dijital kimlik güvenlikleri konularında iyileştirilmesi gerekliliği ortaya çıkmaktadır. Araştırma sonuçları, diğer ülkeler için siber güvenlik seviyelerini ölçmede referans niteliği taşımaktadır.

Neciyev ve Pazarbaşı (2024) çalışmalarında, siber güvenlik ve siber savaş alanında belirledikleri anahtar kelimeler ile bibliyometrik analiz yöntemi uygulamışlardır. Çalışmalarında siber güvenlik alanındaki bilimsel araştırma eğilimlerini analiz etmeyi amaçlamışlardır. Araştırma bulgularında ülkelere göre dağılımlara bakıldığında Amerika Birleşik Devletleri (ABD), Çin, Hindistan, Avustralya ve Birleşik Krallık'ın ilk sıralarda yer aldığı belirtilmiştir.

Siber güvenlik alanında incelenen araştırmalar politika ve strateji üretimi, uluslararası ilişkiler, enerji ve tedarik zinciri gibi birçok alanda çeşitlilik göstermektedir. Bu anlamda çalışmalarda bibliyometrik analiz, uygulama geliştirme yöntemlerine yer verildiği görülmektedir. Araştırmalar ulusal ve uluslararası düzeyde yapılmıştır.

Siber güvenlik, dijitalleşen dünyada ülkelerin ulusal güvenliği açısından stratejik bir alan haline gelmiştir. Türk Dünyası'ndaki ülkeler, benzer dijital tehditlerle karşı karşıya olduklarından, bu alanda yapılan akademik çalışmaların sistemli bir biçimde incelenmesi büyük önem taşımaktadır. Bibliyometrik analiz, belirli bir alandaki örüntüleri, eğilimleri ve etkileri belirlemek amacıyla bilimsel literatür üzerinde yapılan sistematik bir çalışmadır (Passas, 2024). Bibliyometrik analiz yöntemi, siber güvenlik alanındaki yayın eğilimlerini, iş birliği ağlarını ve araştırma boşluklarını ortaya koyarak mevcut durumu değerlendirme ve geleceğe yönelik stratejiler geliştirme imkânı sunmaktadır. Bu çalışma ile siber güvenlik konusunda Türk Dünyası'na yönelik yapılan bibliyometrik analiz ortak akademik ve stratejik adımların planlanmasına katkı sunması anlamında önem arz etmektedir.

3. Yöntem

Bu çalışmada bibliyometrik analiz yönteminden faydalanılmıştır. Bibliyometrik analiz yöntemi, nicel bir araştırma yöntemidir. Bibliyometrik analiz yöntemi, karmaşık bilgi ortamının kavranmasında kullanılan bir analiz tekniğidir (Neciyev ve Pazarbaşı, 2024). Bibliyometrik analiz, büyük hacimli bilimsel verileri keşfetmek ve analiz etmek için kullanılan popüler ve titiz bir yöntemdir. Belirli bir alanın evrimsel nüansların açığa çıkarılmasını sağlarken, bu alandaki yeni alanlara ışık tutar (Donthu ve ark., 2021). Bibliyometrik analiz gerçekleştirilirken; araştırma konusunun belirlenmesi, veri tabanının seçilmesi, anahtar kelimelerin belirlenmesi, verilerin toplanması, bibliyometrik analizin yapılması, görselleştirme, sonuçların yorumlanması ve raporlama adımları uygulanmaktadır (Öztürk ve Kurutkan, 2020).

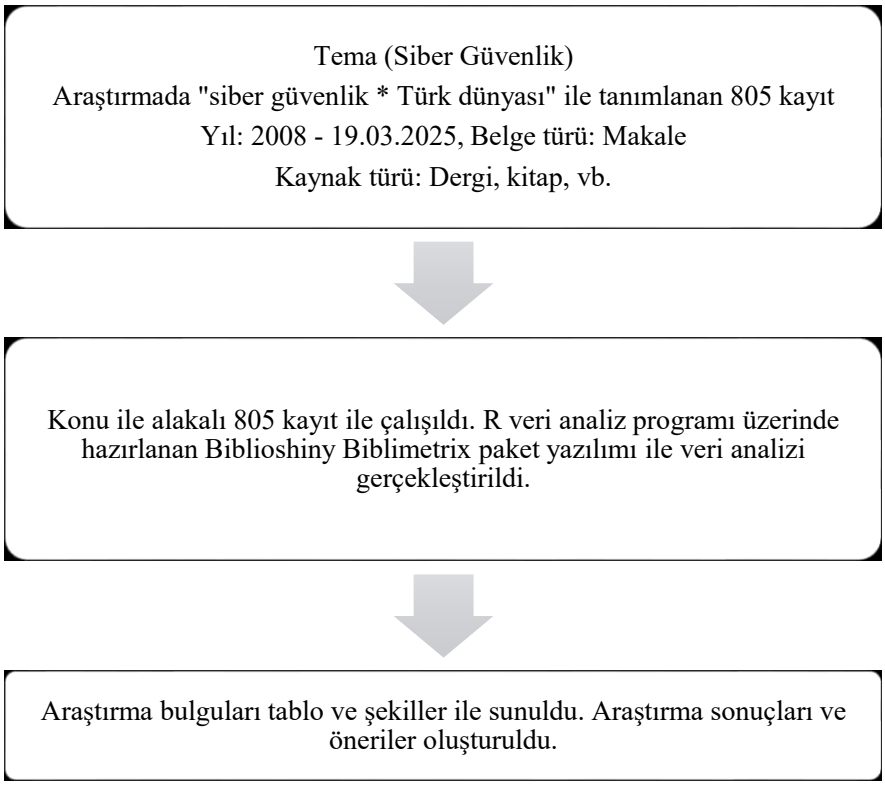
"Dilde, işte, fikirde birlik" anlayışı üzerine temellendirilen Türk Dünyası söyleminin günümüzde dijitalde birleştirilmesi gerekliği kaçınılmazdır. Türk Dünyasının birbirlerini kolaylıkla anlayabilmelerini sağlamaları bu birlik ile mümkün olacaktır (Toker, 2004). Bunu sağlamada siber güvenlik öncelikli konu başlıkları arasında yer almaktadır. Çalışmada, Türk dünyasında siber güvenlik konusunda yayınlanan makalelerin bibliyometrik özelliklerinin belirlenmesi amaçlanmaktadır. Bu kapsamda Web of Science (WOS) veri tabanı üzerinden konu başlığı (topic) "cyber security" olarak arama yapılmıştır. Siber güvenlik (cyber security) bilgi sistemlerini, ağları, cihazları ve verileri yetkisiz erişim, hasar, saldırı veya veri sızıntısı gibi tehditlerden koruma faaliyetlerini ele alırken; siber saldırı (cyber attack) ise bilgi sistemlerine zarar vermek, veri çalmak, hizmeti kesintiye uğratmak veya kontrolü ele geçirmek amacıyla yapılan kötü niyetli dijital eylemleri ele almaktadır. Siber güvenlik (cyber security) ve siber saldırı (cyber attack) kavramları birbirini ilgilendirse de anlam ve amaç açısından tamamen farklıdır. Bu yüzden araştırmaya siber saldırı "cyber attack" kavramı dahil edilmemiştir.

Çalışma kapsamında araştırmaya konu olan makalelere ait kriterler; Türkiye, Azerbaycan, Kırgızistan, Özbekistan ve Kazakistan'da yayınlanmış, makale türünde ve Web of Science indeks filtrelemesi seçilerek belirlenmiştir. 2008-19.03.2025 tarihleri arasında analize ait veriler için arama yapılmıştır (Webofknowledge, 2025). Çalışma, yayınlanmış 805 makaleyi kapsamakta olup, bu verilere bibliyometrik analiz uygulanmıştır. Çalışmada tema için veri toplama süreci ve analiz yöntemi Şekil 1'de özetlenmiştir.

Bibliyometrik analiz ile gerçekleştirilen çalışmada öncelikle siber güvenlik konusunda incelenen 805 makalenin yıllara göre atıf sayıları ve yayınların dağılımlarına ait özellikleri incelenmiştir. Çalışmada yer alan makalelere ait anahtar kelimeler faktör analizi ile yorumlanmıştır. Ayrıca anahtar kelimelere ait trendler de yıllara göre incelenmiştir. Çalışma kapsamında yer alan makalelere ait anahtar kelimelerin ağırlıklı olarak birlikte kullanılmasına yönelik yakınlık ve uzaklıkları faktör analizi sayesinde kümelendirilerek kavramsal yapı haritası oluşturulmuştur. Siber güvenlik çalışmalarına yapılan atıflara ait dağılımlar da değerlendirilmiştir. Analiz için R veri analiz programı üzerinde hazırlanan Biblioshiny Biblimetrix

paket yazılımı kullanılmıştır. Bibliyometrix paket yazılımı açık kaynak kod ile hazırlanmış, geliştirilebilir bir yazılımdır. Ayrıca R Bibliyometrix paketi anahtar kelimelerin tematik haritasını ortaya koyabilmektedir. Bu anlamda diğer programlardan farklılıklara sahiptir. Kategorik temelde kümeleme analizi yöntemleri ile yayın alanları, yazarlar, yayın kaynakları ve ülkeler R programı ve Biblioshiny programı ile görselleştirilmiştir. Görselleştirme sonrası analiz sonuçları ortaya konulmuştur.

Şekil 1: Araştırmaya Ait Veri Toplama Süreci ve Analizi Şeması



Araştırmanın amacı kapsamında aşağıdaki sorulara yanıt aranmıştır:

- Siber güvenlik alanında Türk dünyasında yapılan çalışmaların yıllara göre atıf sayıları dağılımı nasıldır?
- Siber güvenlik alanında Türk dünyasında yapılan çalışmaların anahtar kelime dağılımları nasıldır?
- Siber güvenlik alanında Türk dünyasında yapılan çalışmaların tematik dağılımları nasıldır?
- Siber güvenlik alanında Türk dünyasında yapılan çalışmaların anahtar kelime trendleri nasıldır?
- Siber güvenlik alanında Türk dünyasında yapılan çalışmaların ülke, anahtar kelime ve başlıklara ait üç alan dağılımları nasıldır?

- Siber güvenlik alanında Türk dünyasında yapılan çalışmaların ülkelere göre yoğunluk dağılımları nasıldır?

Araştırma kapsamında öncelikle siber güvenlik konusu teorik olarak ele alınmıştır. Ardından bibliyometrik analiz yöntemi üzerinde durularak siber güvenlik alanında Türk dünyasında yapılan çalışmalar bibliyometrik analiz yöntemiyle değerlendirilmiştir.

4. Bulgular

Çalışmanın bulgular bölümünde, çalışma amacı doğrultusunda bibliyometrik analiz yöntemi ile R veri analiz programı üzerinde hazırlanan Biblioshiny Biblimetrix paket yazılımı kullanılarak Web of Science (WOS) veri tabanında indekslenen çalışmalar kullanılmıştır. Çalışmada araştırma sorularına ilgili yanıtlar aranmıştır. Bu kapsamda yapılan analiz sonucunda elde edilen bulgular değerlendirilmiş, tablo ve grafikler halinde sunulmuştur. Siber güvenlik konusunda Türk dünyasında hazırlanan bibliyometrik çalışmada Tablo 1'de ilgili 2008 – 2025 yıllarına ait toplamda 805 çalışma Web of Science (WOS) veri tabanı üzerinden elde edilmiştir.

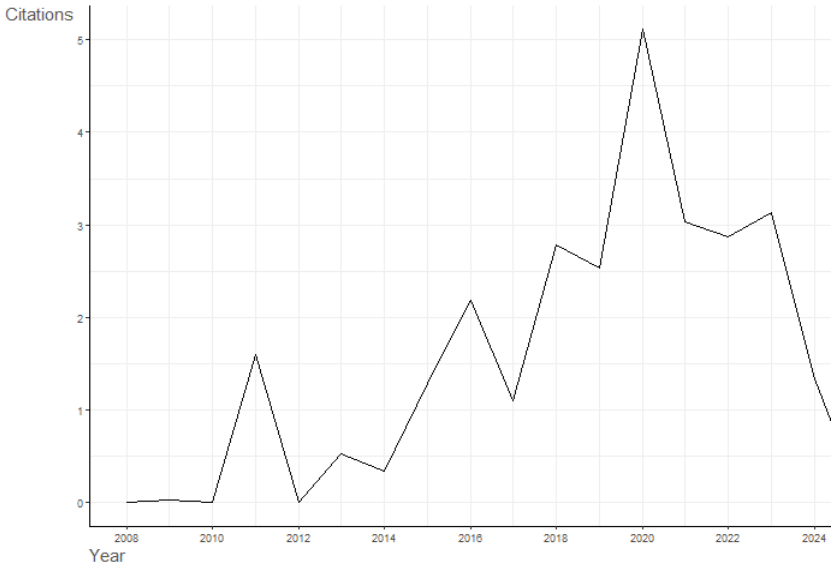
Tablo 1: Bulgulara Ait Genel Özellikler

İncelenen Dönem	2008-2025
Kaynaklar (Dergi, Kitap, vb.)	413
Makale	805
Yıllık Gelişim Oranı %	21,12
Belgelerin Ortalama Yaşı	4,24
Belge Başına Ortalama Atıf Sayısı	12,96
Referanslar	27293
Anahtar Kelimeler	591
Tek Yazarlı Yayınların Sayısı	74
Uluslararası Ortak Yazarlık %	34,79

Tablo 1'de 2008-2025 yıllarına ait toplam 805 makaleye ait bulguların genel özelliklerine yer verilmiştir. 805 adet makale 413 adet farklı kaynakta yayınlanmıştır. Yayın başına ortalama atıf sayısı 12,96 olarak tespit edilmiştir. Uluslararası düzeyde ortak yazarlık oranı % 34,79 olarak bulunmuştur. Toplamda ise 27293 adet referans tespit edilmiştir.

Araştırmanın kapsamında incelenen yıllara ait ortalama yıllık atıf sayılarının dağılımları Şekil 2'de gösterilmiştir.

Şekil 2: Yıllara Göre Atıf Sayıları



Şekil 2'de verilen yıllık atıf sayılarının en yüksek olduğu yıl 2020 yılı olmuştur. 2008-2010 yılları arası ve 2012 yılında atıf sayılarının en düşük oranda oldukları görülmektedir. 2016 yılı itibariyle siber güvenlik alanında artış yaşanması alana olan ilginin arttığı şeklinde yorumlanabilir.

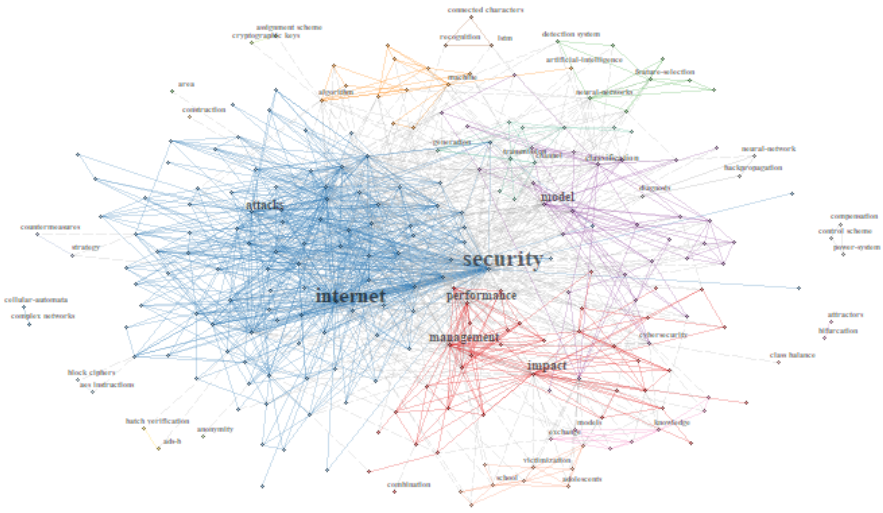
Çalışma kapsamında anahtar kelimeler (keywords plus), makalelerin içeriğinde yer alan sözcük ve sözcük gruplarından toplanan bilgileri içermektedir. Siber güvenlik kapsamında incelenen makalelere ait anahtar kelimeler Şekil 3'te verilmiştir.

Şekil 3: Kelime Bulutu

Şekil 3'te siber güvenlik alanında incelenen 805 makalenin anahtar kelimeleri (keywords plus) kelime bulutunda verilmiştir. Şekil 2'ye göre internet, security (güvenlik) en sık kullanılan kelimeler iken, sistem (system), çerçeve saldırıları (framework attacks), zorluklar (challenges), saldırı tespiti (intrusion detection) ve ağlar (networks) kelimelerinin yüksek sıklıkta kullanıldığı gözlenmektedir.

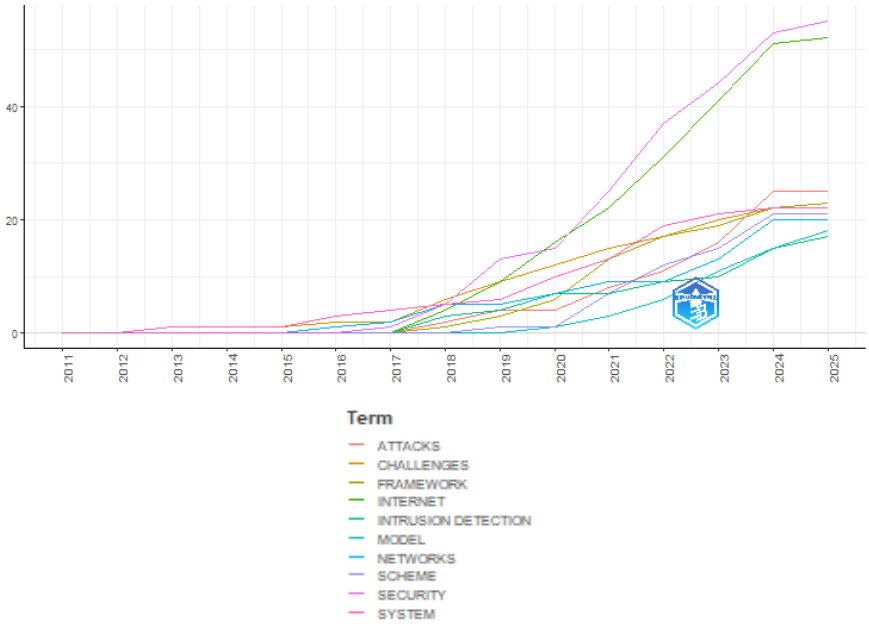
Çalışmada yer alan kavramların anahtar kelime birliktelikleri Şekil 4'te tematik haritada verilmiştir.

Şekil 4: Tematik Harita



Şekil 4' te verilen tematik haritaya göre internet, güvenlik (security), saldırılar (attacks), performans (performance) ve yönetim (management) kelimelerinin birlikte çalışıldığı görülmektedir. Çalışmada kullanılan anahtar kelimelerin yıllara göre kullanım sıklıkları incelenmiştir. Yıllara göre kullanım sıklıkları Şekil 5'te verilmiştir.

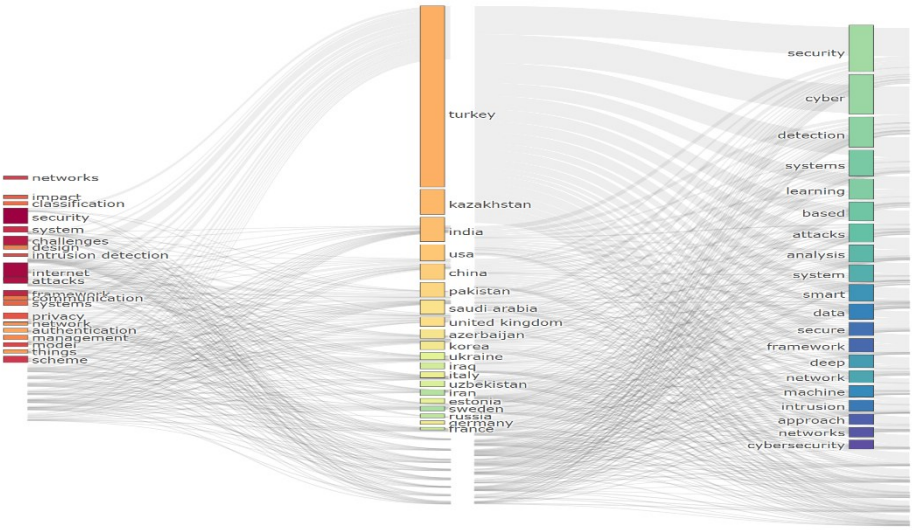
Şekil 5: Anahtar Kelime Trendleri



Şekil 5'te kullanılan anahtar kelimelerin yıllar itibariyle kullanım sıklığı incelenmiş olup, güvenlik (security) kelimesi 2020 yılı itibariyle daha sık kullanılmaya başlanmıştır. 2023 yılından günümüze kadar ise oldukça popüler hale gelmiştir.

İnternet ve saldırı (attack) kelimeleri ise son yıllarda alanda fazla kullanılan kelimeler arasındadır. Ülke, anahtar kelime ve başlıklara ait üç alan ile ilgili verilerin dağılımı Şekil 6'da verilmiştir.

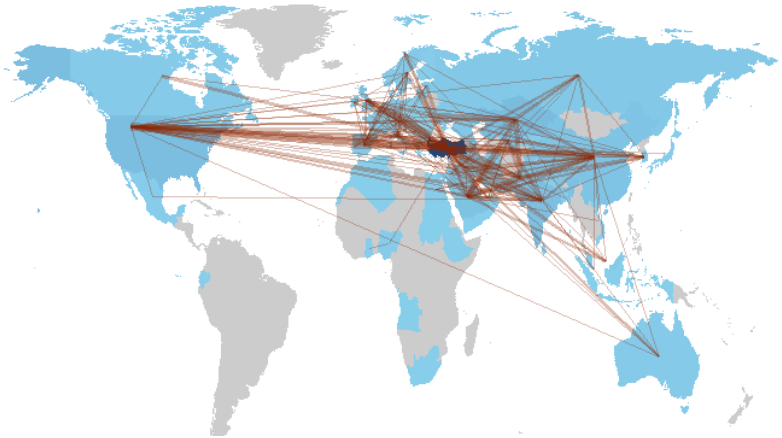
Şekil 6: Ülke, Anahtar Kelime ve Başlıklara Ait Üç Alan Grafiği



Şekil 6'da siber güvenlik alanında yapılan çalışmalarda en fazla Türkiye'de güvenlik (security), siber (cyber) başlıklarında ve ağ bağlantıları (networks), etki (impact) ve sınıflandırma (classification) anahtar kelimelerinde çalışmaların gerçekleştirildiği görülmektedir. Kazakistan, Azerbaycan ve Özbekistan Türkiye'yi takip eden diğer Türk dünyası ülkeleri olmuştur. Bu başlıkta Kırgızistan ise diğer ülkelere göre alt sıralarda yer almıştır.

Siber güvenlik alanında Türk dünyasında yapılan çalışmaların ülkelere ait yoğunlukları Şekil 7'de verilmiştir.

Şekil 7: Ülkelere Ait Yoğunluk Haritaları



Siber güvenlik alanında Türk dünyasında yapılan çalışmaların ülkelere ait yoğunluk haritaları Şekil 7'de gösterilmiştir. Alan ile ilgili en fazla çalışma yapılan ülke Türkiye'dir. Azerbaycan, Kazakistan, Özbekistan, Kırgızistan alana diğer katkı yapan ülkelerdir.

5. Sonuç

Yeni teknolojiler sağladıkları birçok avantajın yanı sıra beraberinde birtakım tehlikeleri de getirmektedir. Siber saldırılar, casusluk ve diğer zararlı yazılımlar ile kişisel güvenliğin yanı sıra ulusal hatta uluslararası sorunlara sebep olunmaktadır. Bu hususta devletlerin kendi sorunlarını çözmeleri ve diğer devletler ile iş birliği içerisinde bulunmaları gerekir. Türk dünyası, başta Türkiye olmak üzere bu çalışmalarını sürdürmekte, bu anlamda pek çok akademik çalışma gerçekleşmektedir.

Siber güvenlik alanında son yıllarda yapılan birçok çalışma uluslararası politikada siber güvenliğin etkin bir araca dönüştüğünü ortaya koymuştur (Bıçakcı, 2014; Güntay, 2018; Güneş, 2019; Çalıkoğlu, 2024; Çifci, 2024). Siber saldırılar, uluslararası düzeyde sivil ve askeri yapılara zarar verebilecek niteliktedir. Siber eylemleri önlemek ve gereken tedbirleri almak adına araştırmacılar tarafından kapsamlı çalışmaların yapılması ve etkili teknik altyapıların oluşturulması zorunluk haline gelmiştir. Türkiye'de Ulusal Siber Olaylara Müdahale Merkezi (USOM) gibi kurumların Türk Dünyası ile etkileşimli şekilde hizmet vermesi siber saldırıları önlemede etkili olacaktır. Türk devletleri nezdinde siber güvenlik alanında düzenleyiciler, kamu ve özel sektör faaliyetleri, devletler arasındaki iş birliğinin artırılması, bilgi işlem teknolojileri alanındaki ortak politikaların geliştirilmesi ile geliştirilmelidir.

Bu çalışma ile siber güvenlik alanında Türk dünyasında yapılan araştırmalar hakkında bilgi sahibi olunması ve ilgili araştırmaların şu ana kadar gelişim seyrinin ortaya konulması amaçlanmıştır. Çalışmanın amacı doğrultusunda bibliyometrik analiz yöntemi ile Web of Science (WoS) veri tabanı temel alınarak ilgili alanda yapılan çalışmalar incelenmiştir. Çalışma kapsamında siber güvenlik ve Türk dünyası konusu teorik olarak ele alınmış, bibliyometrik analiz yönteminden bahsedilmiş, son olarak siber güvenlik alanında Türk dünyasında yapılmış olan çalışmalar bibliyometrik analiz yöntemi ile değerlendirilerek sunulmuştur.

Araştırmada 805 adet kaynak 2008-2025 yılları arasını kapsayacak şekilde bibliyometrik analiz kapsamına alınmıştır. Bu sayede Web of Science (WOS) veri tabanında elde edilen veriler araştırmaların yayın yıllar, yazarlar, ülkeler ve araştırma alanları gibi farklı parametreler kullanılarak analiz çalışması gerçekleştirilmiştir. 2008 yılı itibariyle Türk dünyasında siber güvenlik konulu çalışmalar alanyazında yer almaya başlamıştır. Çalışmaların bu yıllarda başlaması sebebiyle atıf sayılarının da bu yıllarda düşük olması kaçınılmazdır. Son yıllarda teknolojinin her alanda yaygın kullanımı siber güvenlik tehditlerini arttırmakta, Türk dünyası ülkeleri bu alanda araştırmalarını ve atıf sayılarını arttırmaktadır.

Önümüzdeki süreçte de bu sayılarda hızlı artış yaşanacağı öngörülebilir. Ayrıca çalışmada internet, güvenlik, ağ bağlantıları, siber güvenlik kavramları üzerine Türk dünyasında çalışıldığı kelime bulutu, anahtar kelime trendleri ve tematik harita ile gösterilmiştir. Alanyazında bu sonuçları doğrulayıcı çalışmalar ortaya konulmuştur (Önaçan ve Atan, 2016; Aslay, 2017; Acar ve Ulutaş, 2021; Kiraz, 2021).

Türk dünyasında siber güvenlik alanında yapılan çalışmalarda en fazla çalışmanın Türkiye'de gerçekleştirildiği görülmektedir. Kazakistan, Azerbaycan ve Özbekistan Türkiye'yi takip eden diğer Türk dünyası ülkeleri olmuştur. Kırgızistan ise Türk devletleri arasında siber güvenlik konulu çalışmalarda alt sıralarda yer almıştır. Türkiye'nin teknoloji altyapısını her geçen gün ilerlettiği, siber güvenlik konusunda yaptığı çalışmalarla öne çıktığı araştırma sonuçlarında görülmektedir.

Araştırmaya ait birtakım sınırlılıklar mevcuttur. Bu çalışmada elde edilen 805 adet makaleye 19.03.2025 tarihinde ulaşılmıştır. Bu tarihten itibaren veritabanına eklenen yeni makalelere ait yayınların dağılımları, atıf sayıları, yazar ve ülkelere ait bilgiler, anahtar kelimeler ve diğer başlıklara ait değişkenler farklılık gösterebilecektir. Dolayısıyla araştırmacılar tarafından yeni yapılacak çalışmalarda farklı bulguların elde edilmesi mümkündür. Yapılacak yeni çalışmalarda ülke bazlı derinlemesine analizler yapılması önerilebilir. Bu sayede ulusal düzeyde siber güvenlik politikaları ve standartları üzerine çalışmalara katkı sağlanabilecektir. Yine dijital egemenlik ve yerli teknolojiler konu başlıkları ile siber güvenlik alanında iş birliği ve proje geliştirmeye katkı sunacak çalışmalar önerilebilir. Yeni araştırmalara mevcut hukuki altyapıların karşılaştırılması ve uyumlulaştırılması odaklı çalışmaların hem akademik hem de pratik açısından katkı sağlayabileceği ifade edilebilir.

Bu çalışmada seçilen makaleler siber güvenlik alanında Türk dünyasında İngilizce dilinde, makale türünde ve Web of Science (WOS) veri tabanında filtreleme işlemleri ile analiz edilmiştir. Yapılacak yeni çalışmalarda farklı yayın türünde, farklı dillerde ve farklı indekslerde daha kapsamlı şekilde çalışmalar hazırlamaları önerilebilir.

Araştırma ve Yayın Etiği Beyanları

1. Yazar Katkı Beyanı

Bu çalışmada yer alan tüm yazarlar araştırmanın tasarımı, veri toplama, analiz ve yorumlama süreçleri ile makalenin yazımına anlamlı, doğrudan ve özgün katkılarda bulunmuştur. Yazar katkıları şu şekildedir: F.Ç.B: araştırma tasarımı, metodolojinin geliştirilmesi, veri düzenleme ve analiz, makalenin yazımı, gözden geçirilmesi ve düzenlenmesi, danışmanlık. E.P: araştırma tasarımı, metodolojinin geliştirilmesi, veri düzenleme ve analiz, makalenin yazımı, gözden geçirilmesi ve düzenlenmesi. Tüm yazarlar makalenin nihai versiyonunu okuyarak onaylamış ve çalışmanın içeriğine ilişkin ortak sorumluluğu kabul etmiştir.

2. Çıkar Çatışması Beyanı

Yazar(lar), bu çalışmanın hazırlanması, yürütülmesi, veri analizi, sonuçların yorumlanması veya yayımlanması süreçlerinde çıkar çatışmasına yol açabilecek herhangi bir finansal, akademik veya kişisel ilişki ya da çıkar bulunmadığını beyan etmektedir.

3. Etik Beyanı

Bu çalışma, COPE (Committee on Publication Ethics) tarafından belirlenen araştırma ve yayın etiği ilkelerine uygun olarak yürütülmüştür. Araştırma, insan veya hayvan katılımcılar üzerinde herhangi bir deneysel uygulama içermemektedir. Bu nedenle çalışma için etik kurul onayı gerekmemektedir. Çalışmada kullanılan veriler kamuya açık kaynaklardan elde edilmiş veya ikincil veri analizi yöntemiyle değerlendirilmiştir. Araştırmada kullanılan veri ve materyaller, talep doğrultusunda yazarlardan temin edilebilir.

Kaynakça

Acar, S., ve Ulutaş, A. (2021). Türkiye'de siber güvenlik konusunda yazılan lisansüstü tezlerin içerik analizi. *Uluslararası Türk Kültür Coğrafyasında Sosyal Bilimler Dergisi*, 6(1), 93-113.

Acarer, T. (2020). Ülke güvenliğimizde alınabilecek makro siber güvenlik önlemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 6(2), 61-71.

Arslan, M. (2021). Enerji sektöründe siber güvenlik. I. uluslararası Türk enerji birliği kongresi. Almatı, Kazakistan.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies,* 1(1), 24-28.

Aydın, H., Barışkan, M. A., ve Çetinkaya, A. (2021). Siber güvenlik kapsamında enerji sistemleri güvenliğinin değerlendirilmesi. *Güvenlik Bilimleri Dergisi,* 10(1), 151-174.

Bıçakcı, S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler,* 10(40), 101-130.

Çalıkoğlu, C. (2024). Kolektif siber güvenliğin önemi ve Türk devletler teşkilatı. *Kuantum Teknolojileri ve Enformatik Araştırmaları*, 2(1), 1-13.

Çakır, H., ve Taşer, M. (2023). Türkiye'de yapılan siber güvenlik faaliyetlerinin ve eğitim çalışmalarının değerlendirilmesi. *Gazi Üniversitesi Fen Bilimleri Dergisi*, 11(2), 347-366.

Çifci, H. (2024). Cybersecurity maturity of Türkiye: an assessment with enisa's national capabilities assessment framework (NCAF). *Savunma Bilimleri Dergisi*, 20(2), 191-210.

Darıcılı, A. B. (2019). Türkiye'nin siber güvenlik politikalarının analizi; Türkiye'nin potansiyel siber güvenlik stratejisi. *Turkish Journal of TESAM Academy,* 6(2), 11-33.

Deniş, H. E., ve Demircioğlu, F. (2023). Türk dünyası ortak kripto para vizyonu: TDcoin. *MANAS Journal of Social Studies*, 12(2), 786-796.

Dilek, E., Talih, Ö., ve Kaya Bensghir, T. (2023). Estonya 2007 siber saldırılarının incelenmesi ve ülkelerin ulusal siber güvenlik politikalarına etkileri. *Bilgi Yönetimi Dergisi,* 6(2), 332-347.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., ve Lim, W. M. (2021). How to conduct a bibliometric analysis: an overview and guidelines. *Journal of Business Research*, 133, 285-296.

Efe, E., ve Afşar, K. E. (2023). Siber güvenlik ve askerî alanda blok zinciri teknolojisinin potansiyel etkileri: Türk silahlı kuvvetleri örneği. *International Journal of Politics and Security*, 5(2), 101-127.

Erol, M. S., ve Oğuz, Ş. (2018). Karma savaş teorisi ve Rusya-Ukrayna savaşı. *Journal of Turkish World Studies,* 18(2), 399-415.

Gündoğdu, S. (2023). Uluslararası politikada bir etki aracı olarak siber güvenlik ve Türkiye'nin siber güvenlik politikası uygulaması: ulusal siber olaylara müdahale merkezi (USOM). *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33(3), 1325-1337.

Güneş, A. (2019). Küresel güçlerin ulusal siber güvenlik stratejileri: ABD örneği. *Cyberpolitik Journal,* 4(8), 242-258.

Güntay, V. (2018). Siber güvenliğin uluslararası politikada etki aracına dönüşmesi ve uluslararası aktörler. *Güvenlik Stratejileri*, 14(27), 79-111.

Gürdal-Limon, E. (2023). Siber güvenlik açısından savaş yönetim sistemleri ve Türkiye. *Gaziantep University Journal of Social Sciences*, 22(4), 1466-1481.

Hekim, H., ve Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), 135-158.

Karataş, A. (2020). The comparative analysis of national cyber security policies: United States, United Kingdom and Turkey examples. *Academic Social Resources Journal*, 5(19), 737-751.

Kiraz, O. Z. (2021). Siber güvenlik bağlamında yeni tehdit algılamalarının Türkiye'nin güvenlik politikalarına etkileri. *Journal of Management Theory and Practices Research*, 2(2), 69-88.

Kutlu, Ö., Kahraman, S., ve Dinçer, S. (2019). Avrupa Birliği'ne uyum sürecinde Türkiye'nin siber güvenlik politikalarının analizi. *Assam Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı.* https://izlik.org/JA43AM56RK

Neciyev, S., ve Pazarbaşı, B. (2024). Siber güvenlik, siber savaş alanında seçili anahtar kelimeler ile ilgili araştırmaların bibliyometrik analizi. *Gazi Üniversitesi Fen Bilimleri Dergisi,* 12(1), 57-79.

Önaçan, M. B. K., ve Atan, H. (2016). Siber güvenlikte lisansüstü eğitim: deniz harp okulu örneği. *Trakya University Journal of Engineering Sciences,* 17(1), 13-21.

Özdemir, D. M., ve Kantar, G. (2023). Şuşa beyannamesi'nin önemi ve olası etkileri. *MANAS Journal of Social Studies,* 12(2), 733-744.

Özdemir, G. (2025). Uluslararası güvenlikte siber tehditlerin yükselişi ve stratejik savunma politikaları. *Elektronik Sosyal Bilimler Dergisi*, 24(1), 1-20.

Öztürk, N., ve Kurutkan, M. N. (2020). Kalite yönetiminin bibliyometrik analiz yöntemi ile incelenmesi. *Journal of Innovative Healthcare Practices (JOINIHP),* 1(1), 1-13.

Passas, I. (2024). Bibliometric analysis: The main steps. *Encyclopedia,* 4(2), 1014-1025.

Toker, M. (2004). İsmail Gaspıralı ve "Dilde Birlik" fikri üzerine. *Selçuk Üniversitesi Türkiyat Araştırmaları Dergisi,* 16, 31-45.

Uma, M., ve Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security,* 15(5), 390-396.

Webofknowledge. (2025). Web of knowledge search. https://www.webofknowledge.com.

Yanarışık, O. (2020). İç güvenlik ve siber güvenlik. İç güvenlik yönetimi ve polislik. Polis Akademisi Yayınları.

Yayla, M. (2013). Hukuki bir terim olarak "Siber Savaş". *Türkiye Barolar Birliği Dergisi*. 104, 177-202.

Yılmaz, B. A. (2020). Siber terörizm ve değişen istihbarat anlayışı. *Anadolu Strateji Dergisi.* 1(1), 65-81.