Siber Güvenlik Araştırmalarına Küresel Bir Bakış: Yayın Trendleri ve Araştırma Yönelimleri

Araştırma Makalesi/Research Article

Tuğçe KARAYEL[1], Adem AKBIYIK[2]

[1]Yönetim Bilişim Sistemleri, Sakarya Üniversitesi, Sakarya, Türkiye
[2] Yönetim Bilişim Sistemleri, Sakarya Üniversitesi, Sakarya, Türkiye

tugce.aslan2@ogr.sakarya.edu.tr, adema@sakarya.edu.tr

(Geliş/Received:03.05.2023; Kabul/Accepted:21.06.2023)
DOI: 10.17671/gazibtd.1291783

Özet--Makale, Web of Science'ın veritabanında indekslenen siber güvenlik ve bilgi güvenliği araştırmalarının kapsamlı bir bibliyometrik analizini sunmaktadır. Siber güvenlik, son zamanların ilgi odağı olan popüler bir araştırma konusudur. Alandaki küresel araştırma verimliliğini ve gelişimini incelemek için 1980 ve 2021 yılları arasında yayınlanan 4252 makale R tabanlı Biblioshiny paket programı ile analiz edilmiştir. Siber güvenlik alanındaki yayınlanan araştırmalar yıllara göre giderek artan bir eğilim gösterirken bilgi güvenliği ile ilgili olan yayınlar giderek azalan bir eğim göstermiştir. Alanın kavramsal yapısı incelediğinde, son dönemin en dikkat çekici araştırma konuları "siber güvenlik farkındalığı" ve "siber fiziksel sistemler" olduğu bulunmuştur. Ek olarak alanın tematik ağ haritası incelendiğinde bilgi güvenliği teması alanın sosyal boyutunu ifade eden bilgi güvenliği farkındalığı, bilgi güvenliği yönetimi, bilgi güvenliği politikaları, bilgi güvenliği kültürü konularıyla daha çok çalışılmıştır. Siber güvenlik teması ise alanın teknik tarafını ifade eden yapay zeka, büyük veri, blokzincir, makine öğrenmesi ve derin öğrenme gibi konularla daha çok çalışıldığı ortaya çıkmıştır. Çalışmanın bulguları, araştırmacılara, bilgi teknolojisi uzmanlarına ve bilgi uzmanlarına, siber güvenlik alanındaki araştırma ilerlemesine ve yeni araştırma konularını belirlemede yardımcı olabileceği ön görülmektedir.

Anahtar Kelimeler-- siber güvenlik, bilgi güvenliği, bilgi sistemleri güvenliği, bibliyometri, biblioshiny

A Global Perspective of Cybersecurity Research: Publication Trends and Research Directions

Abstract-- The article presents a comprehensive bibliometric analysis of cybersecurity and information security research indexed in the Web of Science database. Cybersecurity is a popular research topic that has been the focus of recent attention in recent times. To examine the global research efficiency and development in the field, 4252 articles published between 1980 and 2021 were analyzed with the R-based Biblioshiny package program. While cybersecurity-related publications have shown an increasing trend over the years, publications related to information security have shown a decreasing trend. When the conceptual structure of the field was examined, the most notable research topics in recent years were found to be "cybersecurity awareness" and "cyber-physical systems. Additionally, when the thematic network map of the field was examined, it was observed that topics related to the social dimension of information security such as information security awareness, information security management, information security policies, and information security culture are studied more. On the other hand, it was revealed that topics related to the technical side of cybersecurity such as artificial intelligence, big data, blockchain, machine learning, and deep learning are studied more. The findings of the study are expected to help researchers, information technology experts, and information professionals in advancing research in the field of cybersecurity and identifying new research topics.

Keywords—cyber-security, information security, information systems security, bibliometry, biblioshiny

1. GİRİŞ (INTRODUCTION)

Kurumların, bireylerin ve toplumların siber saldırılar tarafından tehdit edildiği modern dünyada [1] siber saldırılara karşı mücadele etmek ve saldırıların hızına ayak uydurmak her geçen gün daha da zorlaşmaktadır [2], [3]. Statista'nın hazırlamış olduğu bir rapora göre, dünya nüfusunun yaklaşık %62'si interneti aktif olarak kullanmaktadır [4]. İnternet kullanıcılarının internete erişmek için kullandıkları cihazlar incelendiğinde kullanıcıların neredeyse %91'inin akıllı telefonları kullandığını, %71'inin laptop ve/veya masaüstü bilgisayarlarını, %30'unun akıllı TV'leri ve %14'ünün diğer akıllı ev cihazlarını kullandığını bulunmuştur [5]. İnternete bağlanan bilgi işlem cihazlarının artmasıyla güvenlik sorunları da artmaktadır [6]. Genel olarak küresel internet kullanıcılarının yarısından fazlası siber saldırı yaşamıştır [7]. Operasyonel teknoloji saldırıları yıldan yıla %2.000 artmaktadır [8]. Siber güvenlik, siber saldırıları önlemeye yardımcı olabileceği için şu anda geniş bir paydaş yelpazesinde büyük ilgi gören ve dikkat çeken, sonuçları ve etkileri küresel olan bir alandır [9]. Bu nedenle, söz konusu bu alandaki bibliyometrik değerlendirmelerin yapılması büyük önem taşımaktadır.

Çalışmanın amacı, siber güvenlik ile ilgili alan dinamiklerini ve son araştırma eğilimlerini ortaya koymaktır. Makalede araç olarak Web of Science Core Collection veri tabanı kullanılmıştır. Web of Science Core Collection veri tabanından elde edilen veriler, siber güvenlik alanının zaman içinde gelişimini detaylı bir şekilde inceleme imkânı sunmakta ve konuyla ilgili bilimsel haritalamayı ortaya çıkarmaktadır. Çalışmanın amacı, siber güvenlik ile ilgili alan dinamiklerini ve son araştırma eğilimlerini ortaya koymaktır. Bu amaç doğrultusunda alanın performans göstergeleri, kavramsal ve tematik yapısı incelemek ve anlamak için bibliyometrik analiz yapılmıştır. Bu araştırmacının amacı doğrultusunda aşağıdaki sorulara cevap aranacaktır;

- Siber güvenlik ile ilgili yayınların kavramsal yapısı nasıldır ve ön plana çıkan unsurlar nelerdir?
- Siber güvenlik ile ilgili yayınların performans göstergeleri nelerdir? (En çok katkı sunan yayınlar, dergiler, ülkeler, atıf alan yazarlar)
- Siber güvenlik ile ilgili yayınların tematik gelişim haritasında ön plana çıkan unsurlar nelerdir?

Araştırma sonuçlarının siber güvenlik alanına ve ilgili alanda çalışan araştırmacılara günümüz ve geleceğe dair ipuçları sunarak katkı sağlayacağı düşünülmektedir.

Siber güvenlik ile ilgili farklı ülkelerden yazarlar tarafından alanın mevcut yapısının derinlemesine incelenmesini sağlayan bibliyometrik çalışmalar yapılmıştır. Tablo 1'de literatürde hangi çalışmaların yapıldığı, arama stratejisi ve yıl aralığı gibi detaylı bilgiler paylaşılmaktadır.

2. LİTERATÜR İNCELEMESİ (LITERATURE REVIEW)

2.1. Siber Güvenlik (Cyber Security)

Dijital çağda kurumlardaki bilgisayarlarda ve diğer cihazlarda depolanan veri miktarları çok büyük boyutlara ulaşmıştır. Artan veri miktarı beraberinde güvenlik sorunlarını da getirmiştir. Siber güvenlik küresel bir sorundur ve uzmanlar, gün geçtikçe artan güvenlik sorunu ile karşı karşıya kalmaktadır [10]. Siber güvenlik için farklı ve birçok tanımlama vardır, bunlardan biri de Kaspersky'nin tanımıdır. Kaspersky siber güvenliği, bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü niyetli saldırılara karşı koruma uygulaması olarak tanımlamaktadır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir [11], [12]. Uluslararası Telekomünikasyon Birliği (ITU) siber güvenliği şu şekilde tanımlamaktadır: Siber güvenlik, organizasyonu ve kullanıcı varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin bütünüdür [13]. Organizasyon ve kullanıcının varlıkları, bilgi işlem cihazlarını, personeli, altyapıyı, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen veya depolanan verileri/bilgileri içermektedir. Başka bir tanımlamaya göre ise, siber güvenlik, siber ortamdaki ilgili güvenlik risklerine karşı kuruluşun ve kullanıcı varlıklarının güvence altına alınmasını ve bu güvencenin sürdürülmesini sağlamaya çalışır [14]. Kısaca siber güvenlik, bilgi işlem cihazlarını veya kullanıcı varlıklarını yetkisiz erişime veya saldırılara karşı korumak için alınabilecek güvenlik önlemlerinin bütünü olarak tanımlanmaktadır [2].

Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinen siber güvenliğin temel amacı, işletmenin bilgi teknolojileri altyapısını ve günlük operasyonları için gerekli bilgilerini korumaktır. Kurumlar için siber güvenlik, bilgisayar güvenliği, bilgi güvenliği, bilgi sistemleri güvenliği gibi çeşitli biçimlerde ele alınabilmektedir. Güvenli bir bilgisayar sistemi, bilgilerin gizliliğini, kullanılabilirliğini ve bütünlüğünü sağlamalıdır. Bilgisayar sisteminin güvenliği, yetkisiz kişi veya program aracılığıyla bilgisayara veya ağa zarar vermek veya normal faaliyet akışını bozmak amacıyla tehlikeye girebilir [2]. Söz konusu bu tehlikeleri yok etmek için siber güvenlik sağlanmalıdır.

2.2. Siber Güvenlik ve Bibliyometrik Analiz (Cyber Security and Bibliometric Analysis)

Tablo 1. Siber Güvenlik ve Bibliyometrik Analiz ile İlgili Yayınlar
(Publications on Cyber Security and Bibliometric Analysis)

Yazar	**Zaman Aralığı**	**Kaynak**	**Yayın Sayısı**	**Arama Stratejisi**
Jalali ve ark.(2019)	1966-2017	Web of Science ve Pub Med	472	"Health*" AND "Cybersecurity" OR "Cyber Security" OR "Cyber Attack*" OR "Cyber Crisis*" OR "Cyber Incident*" OR "Cyber Infrastructure*" OR "Cyber Operation*" OR "Cyber Risk*" OR "Cyber Threat*" OR "Cyberspace*" OR "Data Breach*" OR "Data Security*" OR "Firewall*" OR "Information Security*" OR "Information Systems Security*" OR "Information Technology Security*" OR "IT Security*" OR "Malware*" OR "Phishing*" OR "Ransomware*" OR "Security Incident*" OR "Information Assurance*"
Taylor ve ark.(2020)	2015-2018	IEEE, ScienceDirect, SpringerLink, ACM Digital Library, Google Scholar	655	"blockchain" OR "block-chain" OR "distributed ledger" AND "cyber Security" OR "cybersecurity" OR "cyber-Security"
Rahim (2021)	2003-2020	Scopus	606	"cyber threat*, cyberthreat*, cyber-threat*, cyber attack*, cyberattack*, and cyber-attack*"
Elango ve ark. (2022)	1999-2020	Web of Science ve Scopus	989	"CyberSecurity" OR "Cyber Security" OR "Cyber-Security" OR "Cyber incident management" OR "Cybersafety" OR "Cyber crisis management" OR "Cyber defense" OR "Cyber threat management" OR "Cyber Safety"
Loan ve ark.(2022)	2011–2020	Web of Science	1171	"CyberSecurity" OR "Cyber-Security" OR "Computer Security" OR "Information security" OR "Web Security" OR "Network Security" OR "Internet safety"
Sharma ve ark. (2023)	2011–2021	Web of Science	9152	"online" AND "fraud" OR "anomaly" OR "malware" AND "detection" OR "cyber" AND "forensics" OR "attack" AND "machine OR deep" AND learning"
Bu makale	***1980-2021***	***Web of Science***	***4252***	***"Cyber Security" OR "cybersecurity" OR "cyber-Security" OR "Informations systems Security" OR "Informations technology Security" OR "IT Security" OR "Information security" OR "computer Security"***

Jalali ve ark. (2019) siber güvenlik ve sağlık hizmetlerinin bibliyometrik bir analizini sunmaktadır. Çalışma, siber güvenlikle ilgili makalelerin çoğunun teknolojiye odaklandığını göstermektedir. Kümeleme analizlerinde, teknoloji odaklı makaleler tüm kümelerin yarısından fazlasını oluştururken, yönetim makaleleri yalnızca %32'sini oluşturduğu bulunmuştur. Siber güvenliğin teknolojik yönlerine odaklanan çalışmaların sayıca çok olması, teknolojik olmayan değişkenlerin (insan temelli ve organizasyonel yönler, strateji ve yönetim) yeterince incelenmediğini göstermektedir [13]. Taylor ve ark. (2020) blokzincir ve siber güvenlik temalarının bibliyormetrik incelemesini çalışmıştır. Bu araştırmada en dikkat çekici bulgu, blok zincir ve siber güvenlik uygulamalarına ilişkin tüm çalışmaların neredeyse yarısının (%45) IoT cihazlarının güvenliği ile ilgili olduğu bulunmuştur. İkinci sıradaki en popüler tema ise veri depolama ve paylaşma bulunmuştur [16].

Rahim (2021) siber tehditler ve siber saldırılar üzerine bibliyometrik bir inceleme gerçekleşmiştir. Bu çalışma sonuçlarına göre, siber saldırılar ve siber tehditlerle ilgili literatürün yazarlığı ve küresel dağılımında ABD'nin yazarlık açısından en fazla yayına ve etkiye sahip olduğu, gelişmekte olan ülkelere odaklanan araştırma sayısının az olduğu bulunmuştur[17]. Elango ve ark. (2022) Hindistan'da yayınlanan siber güvenlik çalışmalarına odaklanmıştır. Bu araştırmada 989 makale incelenmiş olup bu makalelerde en çok araştırılan anahtar sözcükler kriptografi, akıllı şebeke, güvenlik, ağ güvenliği, bulut bilişim, makine öğrenimi ve saldırı tespiti olmuştur [18]. Loan ve ark. (2022) siber güvenlik ile ilgili toplamda 1171 çalışma ile

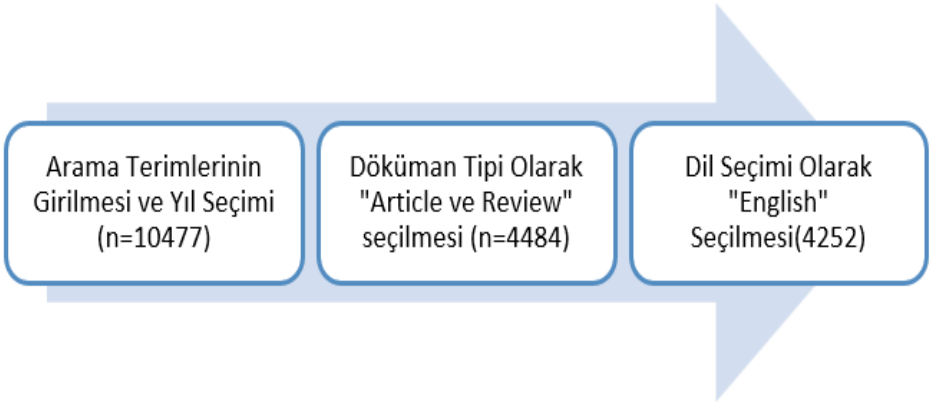
bibliyometrik analiz yapmıştır. Bu çalışma sonuçlarına göre alandaki küresel dağılımındaki en yüksek payı ABD 'nin aldığı bulunmuştur [19]. Sharma ve ark. (2023) siber güvenlik ve siber adli tıp alanlarında yazarlar, dergiler, ülkeler, anahtar kelimeler, kaynaklar ve makaleler açısından bibliyometrik analiz gerçekleştirmiştir. Araştırma sonuçlarına göre "Kötü amaçlı yazılım algılama" anahtar kelimesi, 2012-2018 döneminde en çok araştırılan anahtar kelime olduğu tespit edilmiştir. Siber güvenlik ve siber adli tıp alanında en çok araştırma yayınlayan dergi ise "IEEE Access" dergisi olmuştur [20].

3. YÖNTEM (METHODOLOGY)

3.1. Veri Kaynakları (Data Sources)

Bu çalışmada Web of Science'ın veritabanında indekslenen siber güvenlik ve bilgi güvenliği konularında yayınlanan makaleler bibliyometrik analiz yöntemiyle incelenmektedir. Bibliyometri, herhangi bir alan ile ilgili yayımlanmış araştırmaları nicel olarak analiz etmek için matematiksel ve istatistiksel yöntemler kullanan disiplinler arası bir disiplindir. Bir alanın gelişimi ve eğilimleri bibliyometrik analiz yöntemle ile incelenmektedir. Görselleştirme araçları ile değerli bilgileri çıkarmak için veri madenciliği tekniklerini kullanırken aynı zamanda elde edilen bilgileri farklı boyutlarda görüntülenmesini sağlamaktadır. Elde edilen analiz sonuçlarına göre alandaki akademik üretkenliği değerlendirmek, alandaki önemli konuları özetlemek ve eğilimleri tahmin etmek mümkündür [21]. Bibliyometrik analizlerden performans analizi, kavramsal yapı ve tematik gelişim haritası gerçekleştirilmiştir. Verilerin elde edilme aşamaları şu şekilde gerçekleşmiştir;

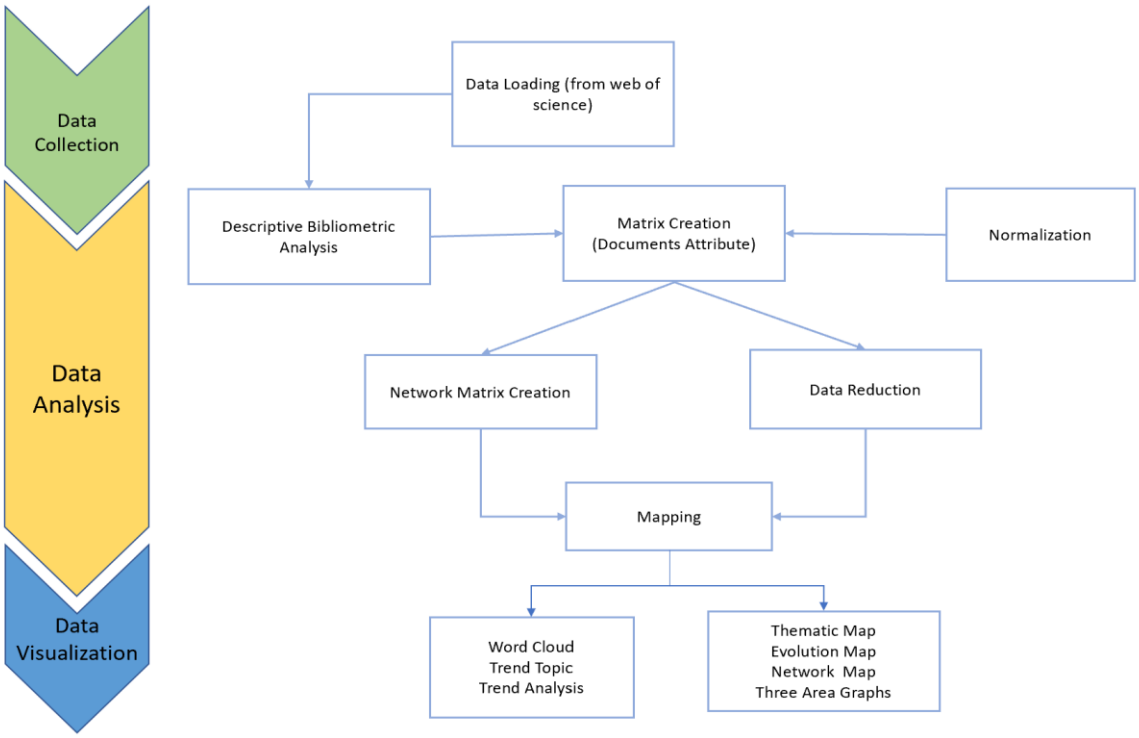
İlk olarak, WOS veri tabanından "Title" sekmesinde "cyber security" OR "cybersecurity" OR "cyber-security" OR "informations systems Security" OR "informations technology security " OR "IT security" OR "information security" OR "computer security" terimleri ile yapılan aramada 1980-2021 yılları arası analize dâhil edilmiş olup toplamda 10.477 yayın bulunmuştur. Veri tabanına 11 Haziran 2022'de erişilmiştir ve eksik veri seti nedeniyle 2022 yılı hariç tutulmuştur. İkinci olarak, doküman tipi olarak "Article" ve "Review Article" seçilmiştir. Toplamda yayın sayısı 4484'e düşmüştür. Son olarak ise, dil kategorisinden "English" dili seçilmiş olup yayın sayısı 4252 olmuştur (Şekil 1).



Şekil 1. Araştırma Verilerinin Elde Edilmesinde İzlenen Yol Haritası
(Roadmap for Obtaining Research Data)

3.2. Veri Analizi (Data Analysis)

Standart bibliyometrik analiz süreci üç adım içerir; veri toplama, veri analizi, veri görselleştirme (Şekil 2). Bibliometrix yazılım paketi, Profesör Massimo Aria tarafından 2017 yılında R diline dayalı olarak geliştirilmiş bir bibliyometrik yazılım paketidir. Scopus veya Web of Science veritabanlarından alınan makaleler üzerinde istatistiksel analiz, veri ön işleme, birlikte oluşum matrisi oluşturma, ortak alıntı analizi, eşleştirme analizi, eş kelime analizi ve küme analizi gibi çeşitli analizler gerçekleştirilebilmektedir. Çeşitli bilimsel haritalama araçlarının görselleştirme yeteneklerini birleştiren bibliometrix, literatür hakkında detaylı bilgi analizine ve sonuçların görselleştirilmesine olanak sağlar. Massimo Aria, R dili yazılım paketi kullanarak Bibliometrix'in ikinci bir sürümü olan biblioshiny uygulamasını geliştirmiştir. İki yazılım arasındaki fark, "bibliometrix" çalışma modunun kod komutlarından oluşması, "biblioshiny" ise kullanıcıların etkileşimli bir web arayüzü üzerinde ilgili bibliyometrik ve görsel analizler yapmasına izin veren kod komutlarına ihtiyaç duymayan bir programdır. Biblioshiny kullanıcının bilgi giriş yoğunluğunu ve program kullanımını büyük ölçüde kolaylaştırmaktadır [22]. Bu makalede, siber güvenlik alanındaki araştırma durumunu ve araştırma eğilimlerini analiz etmek ve görselleştirmek için bibliometrix ve biblioshiny yazılım paketleri kullanılmıştır. Web of Science veritabanından elde edilen veri seti R (4.0.3.) programı (paket olarak kurulan Bibliyometrix ve biblioshiny) ile analizi yapılmıştır. Analiz aşamasında ilk olarak bibliometrix R paketi R Studio aracılığıyla kurulmuş ve yüklenmiştir. Daha sonra R programlama konsolunda "*bibliometrix::biblioshiny()*" komutu girilerek biblioshiny uygulaması başlatılmıştır. Son olarak veri dosyası Biblioshiny arayüzüne yüklenmiştir. Daha sonra çalışmanın amacına ve araştırma sorularına uygun olan analizler gerçekleştirilmiştir.



Şekil 2. Bibliyometrik Analiz Süreci
(Bibliometric Analysis Process)

4. BULGULAR (FINDINGS)

Bu bölümde siber güvenlik alanının genel yapısını ve kavramsal yapısını ortaya koymak adına literatürde bu konu üzerine yazılmış 4252 yayına ait analiz sonuçlarına yer verilmiştir. Alandaki yayınların, dergilerin, araştırmacıların ve ülkelerin performans analizleri, alanının entelektüel yapısını keşfetmek için, siber güvenlik araştırmalarının tematik gelişimi, araştırma, odakları ve güncel trendleri tespit edilmiştir.

4.1. Siber Güvenlik ile İlgili Yayınların Performans Göstergeleri (Performance Indicators of Publications Related to Cyber Security)

Siber güvenlik ve bilgi güvenliği teması altında en fazla atıf alan 10 yayının bilgileri Tablo 2' de yer almaktadır. Bu bulgulara göre en fazla atıf alan yayının (n=933) Buczak ve arkadaşları tarafından 2016 yılında IEEE Communications Surveys & Tutorials dergisinde yayımlanan "A Survey of Data Mining and Machine Learning Methods For Cyber Security Intrusion Detection" adlı çalışma olduğu görülmektedir. Bu çalışmada, saldırı tespitini sağlayan makine öğrenimi ve veri madenciliği yöntemlerine yönelik bir literatür araştırması yapılmıştır. Her iki yöntem içinde siber saldırı tespit sorunlarına yönelik çeşitli uygulamaları açıklanmıştır. Farklı makine öğrenimi/veri madenciliği algoritmaları tanıtılmış ve bu yöntemler için bir dizi karşılaştırma kriteri sunulmuştur. Ayrıca, makale çözülmesi gereken siber sorunun özelliklerine bağlı olarak kullanılacak en iyi yöntemler hakkında öneriler sunmaktadır [23]. Bu çalışmaya atıf veren makaleler incelendiğinde ise genelde saldırı tespiti, anomali tespiti ve saldırı tespit sistemi konularını ele alan teknik araştırmalar olduğu görülmüştür. En çok atıf alan ikinci yayın (n=762) Bulgurcu ve ark. tarafından 2010 yılında MIS Quarterly dergisinde yayımlanan "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness" başlıklı çalışmadır. Bu çalışma, bir kuruluşun çalışanlarının bilgi güvenliği politikasına uyumluluğunun öncüllerini araştırmıştır. Planlı davranış teorisine dayanarak, normatif inanç ve öz-yeterlik ile birlikte, bir çalışanın uyumluluğa yönelik tutumunun bilgi güvenliği politikasına uyma niyetini etkileyip etkilemediğine bakılmıştır. Ayrıca, bilgi güvenliği farkındalığının bir çalışanın bilgi güvenliği politikası ile uyumluluğuna yönelik tutumu üzerindeki etkisini de araştırılmıştır. Çalışma sonuçlarında, bir çalışanın bilgi güvenliği politikasına uyma niyetinin, tutum, normatif inançlar ve öz yeterlilikten önemli ölçüde etkilendiğini bulunmuştur [24]. Bu makaleye atıf veren çalışmalar incelediğinde genellikle bilgi güvenliği politikası, koruma motivasyon teorisi, bilgi güvenliği farkındalığı ve bilgi güvenliği politikası uyum gibi daha çok sosyal konuları araştıran makaleler olduğu görülmüştür.

En çok atıf alan üçüncü çalışma (n=553) Wang & Lu (2013) tarafından Computer Networks dergisinde yayımlanan "Cyber Security in The Smart Grid: Survey and Challenges" başlıklı araştırmadır. Bu yazıda, akıllı şebeke için siber güvenlik sorunlarına odaklanmış olup özellikle, akıllı şebekelerdeki güvenlik gereksinimlerini,

ağ açıklarını, saldırı karşı önlemlerini , güvenli iletişim protokollerini ve mimarilerini incelenmiştir [25]. Bu araştırmanın atıf ağı incelendiğinde akıllı şebekeler, akıllı sayaçlar, siber fiziksel sistemler, kimlik doğrulama konuları ön plana çıkmaktadır.

Dördüncü sıradaki çalışma, Johnston ve Warkentin (2010) tarafından MIS Quarterly dergisinde yayımlanan " Fear Appeals and Information Security Behaviors: An Empirical Study" çalışmadır. Bu çalışma, korku çekiciliğinin, tehditlerin azaltılmasına yönelik belirli bilgisayar güvenlik eylemlerini uygulamada son kullanıcıların uyumu üzerindeki etkisini araştırmak içindir. Teknoloji benimseme ve korku çekiciliği teorilerinin bir karışımını temsil eden kavramsal bir model test edilmiştir. Çalışma sonuçlarına göre, korku çekiciliğinin, önerilen bireysel güvenlik eylemlerine uyma konusundaki son kullanıcı davranışsal niyetlerini etkilediği bulunmuştur [26]. Bu makaleye atıf veren çalışmalar incelediğinde genellikle koruma motivasyon teorisi, uyum, planlı davranış teorisi, bilgi güvenliği politikası gibi sosyal konuları çalışan makaleler olduğu görülmüştür.

En çok atıf alan beşinci çalışma (n=507) Jain ve ark.(2006) tarafından IEEE Transactions on Information Forensics and Security dergisinde yayımlanan "Biometrics: A Tool For Information Security" başlıklı araştırmadır. Bu yazıda, bir kişiyi fiziksel veya davranışsal özelliklerine göre tanıma bilimi olarak tanımlanan biyometri bilgi güvenliği açısından incelenmektedir. Biyometrik taramanın bilgi güvenliği ile ilgili sorunların çözümleri, biyometrik sistemlerin karşılaştığı temel zorluklar, büyük ölçekli kimlik doğrulama sistemlerinde ölçeklenebilirlik ve güvenlik sorunlarına ilişkin çözümler tartışılmaktadır[27]. Bu araştırmanın atıf ağı incelendiğinde yüz tanıma, parmak izi tanıma, göz tanıma, kimlik doğrulama konuları ön plana çıkmaktadır.

Puhakainen ve Siponen (2010) tarafından MIS Quarterly dergisinde yayımlanan "Improving Employees' Compliance Through Information Systems Security Training:" başlıklı çalışma atıf sıralaması tablosuna göre altıncı sırada yer almaktadır (n=506). Bu çalışmada, iki teoriye dayanan bir eğitim programı önerilmektedir. Bilgi sistemleri güvenlik politikası uyum eğitimi için eğitim programı eylem araştırması projesi yapılmıştır. Eylem araştırması, teoriye dayalı eğitimin olumlu sonuçlar verdiğini göstermiştir. Çalışma sonuçlarında eğitim uygulamasında çalışanları motive eden içerik ve yöntemlerin kullanılması gerektiği önerilmektedir. Ek olarak bu çalışma, çalışanların bilgi sistemleri güvenlik politikası uyumluluğunu iyileştirmek için sürekli bir iletişim sürecinin de gerekli olduğunu ortaya koymuştur [28].

En çok atıf alan yedinci çalışma (n=375) Herath ve Rao (2009) tarafından Decision Support Systems dergisinde yayımlanan "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness" başlıklı araştırmadır. Bu çalışmada, çalışanların bilgi güvenliği politikalarına uyumu konusunda cezaların teşvik edici etkileri üzerine teorik bir model önerilmektedir. Çalışma sonuçlarına göre, güvenlik davranışlarının hem içsel hem de dışsal motivasyonlardan etkilendiğini göstermektedir. Öznel normlar ve akranlar tarafından uygulanan baskılar, çalışanların bilgi güvenliği davranışlarını etkilemektedir. Fakat cezanın güvenlik davranış niyetlerini olumsuz etkilediği bulunmuştur [29].

En çok atıf alan sekizinci çalışma (n=354) Yan ve ark. (2012) tarafından IEEE Communications Surveys & Tutorials dergisinde yayımlanan "A Survey On Cyber Security For Smart Grid Communications" başlıklı araştırmadır. Bu çalışma, akıllı şebeke iletişim sistemlerindeki güvenlik açıklarının ve potansiyel siber saldırıların bir özetini sunmaktadır. Ayrıca, akıllı şebeke iletişim sistemlerinde siber güvenliğin başlıca zorluklarını ve mevcut çözümlerini tartışmaktadır [30].

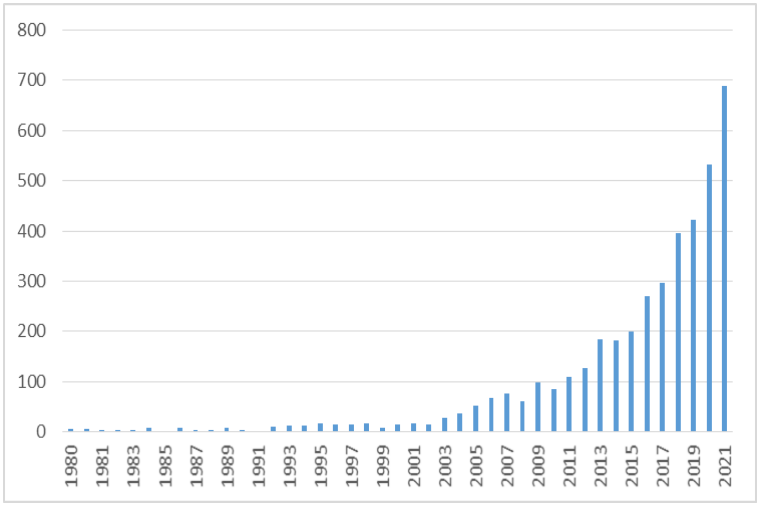
Crossler ve ark. (2013) tarafından Computers & Security dergisinde yayımlanan "Future Directions For Behavioral Information Security Research" başlıklı çalışma atıf sıralaması tablosuna göre dokuzuncu sırada yer almaktadır (n=331). Bu makalede, davranışsal bilgi güvenliği araştırma alanı için karşılaşılan zorluklar ve gelecekteki yönelimleri literatür taraması yöntemiyle açıklanmıştır [31].

Ifinedo (2012) tarafından Computers & Security dergisinde yayımlanan "Understanding Information Systems Security Policy Compliance: An Integration of The Theory of Planned Behavior and The Protection Motivation Theory" başlıklı çalışma atıf sıralaması tablosuna göre onuncu sırada yer almaktadır (n=324). Bu araştırmada, planlı davranış teorisi ve koruma motivasyon teorisinden yararlanılarak bilgi sistemleri güvenlik politikasına uyumluluğu test eden bir model önerilmiştir. Anket, işletme yöneticisi ve bilgiişlem uzmanı olan 124 kişiye uygulanmıştır. Çalışma sonuçlarına göre, öz yeterlilik, uyumluluğa yönelik tutum, öznel normlar, yanıt etkinliği ve algılanan güvenlik açığı faktörlerinin çalışanların bilgi sistemleri politikasına uyum niyetlerini olumlu yönde etkilediği bulunmuştur. Fakat algılanan önem ve yanıt maliyeti faktörleri çalışanların bilgi sistemleri politikasına uyum niyetleri üzerindeki etkisi bulunamamıştır [32].

Tablo 2. En Çok Atıf Alan Yayınlar
(Most Cited Publications)

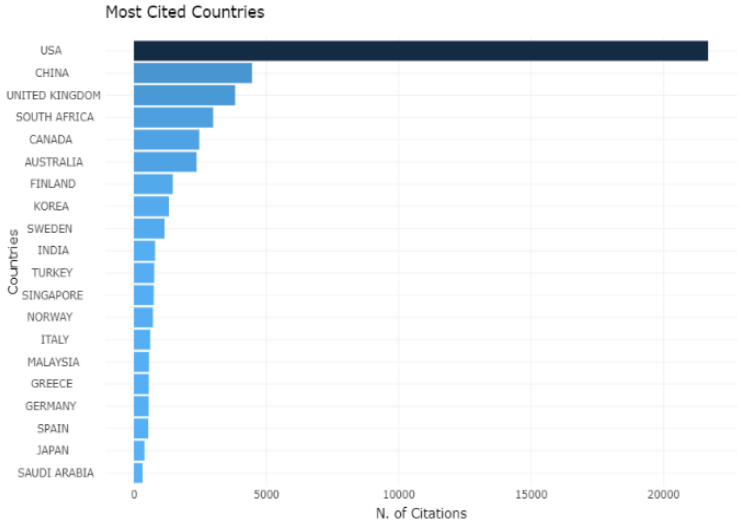
Nu	Yazar	Dergi	Yıl	Başlık	Atıf
1	Buczak ve ark.	Ieee Commun Survey Tut.	2016	A Survey of Data Mining and Machine Learning Methods For Cyber Security Intrusion Detection	933
2	Bulgurcu ve ark.	MIS Quarterly	2010	Information Security Policy Compliance: An Empırıcal Study of Ratıonalıty-Based Belıefs and Information Security Awareness	762
3	Wang ve Lu	Comput Netw.	2013	Cyber Security in The Smart Grid: Survey and Challenges	553
4	Johnston ve ark.	MIS Quarterly	2010	Fear Appeals and Information Security Behavıors: An Empırıcal Study	540
5	Jaın ve ark.	Ieee T Inf. Foren Sec.	2006	Biometrics: A Tool For Information Security	507
6	Sıponen ve ark.	Mıs Quarterly	2010	Improvıng Employees' Compliance Through Information Systems Security Traınıng	506
7	Herath ve ark.	Decision Support Systems	2009	Encouraging Information Security Behaviors In Organizations: Role Of Penalties, Pressures and Perceived Effectiveness	375
8	Yan ve ark.	Ieee Commun. Surv. Tut.	2012	A Survey on Cyber Security For Smart Grid Communications	354
9	Crossler ve ark.	Computer Security	2013	Future Directions For Behavioral Information Security Research	331
10	Ifinedo P.	Computer Security	2012	Understanding Information Systems Security Policy Compliance: An Integration of The Theory of Planned Behavior and The Protection Motivation Theory	324

Şekil 3 1980 – 2021 yılları arasında yıllara göre yayın sayısını sunmaktadır. Buna göre, bu konudaki yayınlar 2015 yılı itibariyle ivme kazanmış ve 2021 yılında bu alanla ilgili 688 çalışma yayınlanmıştır. Son 5 yılda toplam yayın sayısının yarısından fazlasının yayımlandığı gözlenmektedir. Son yıllarda, özellikle dijital dönüşümün yaygınlaşması beraberinde siber güvenlik konusuna olan ilgiyi de artmıştır. Bu nedenle, hakemli yayınlardaki artış, araştırmacılara ve diğer paydaşlara etkileri olan küresel bir araştırma alanına işaret etmektedir.



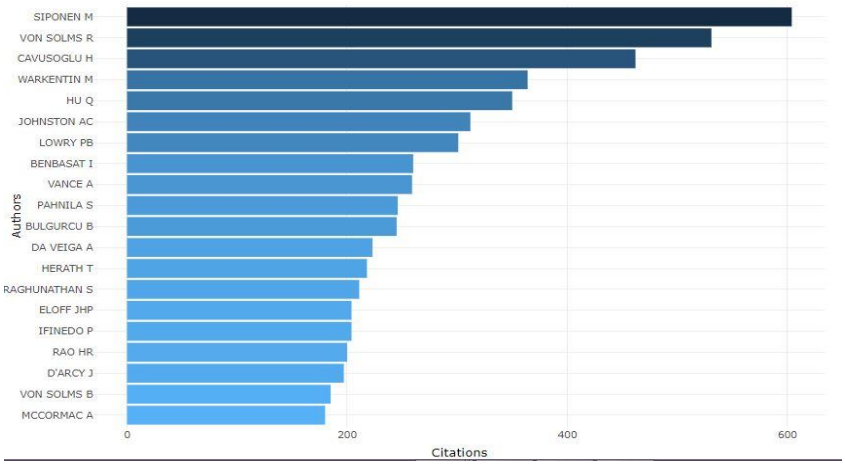
Şekil 3. Yıllara Göre Yayın Sayısı
(Number of Publications by Years)

Şekil 4' te en çok yayın yapan 20 ülke atıf alma sırasına göre listelenmiştir. Bu bağlamda siber güvenlik konusunda en çok atıf alan ülke sıralamasında birinci sırada yer alan ABD yaklaşık 20000 atıf almıştır. Bilgisayar biliminin menşe ülkesi olan ABD [33] ile diğer ülkeler arasındaki atıf sayısı farkı oldukça fazladır. ABD siber güvenlik ve bilgi güvenliği konusunda yapılan çalışmalarla küresel çapta lider olduğu Şekil 2'den anlaşılmaktadır. Atıf sıralamasında ikinci sırada 4458 atıf sayısıyla Çin olduğu görülmektedir. Bu ülkeleri sırasıyla Birleşik Krallık, Güney Afrika ve Kanada ülkeleri takip etmektedir. Türkiye ise on birinci sırada yer almaktadır.



Şekil 4. En Çok Atıf Alan Ülkeler
(Top Cited Countries)

Siber güvenlik araştırmalarına uluslararası yazarlar da dâhil olmak üzere toplam 8736 yazar katılmıştır. Şekil 5'te siber güvenlik çalışmalarına yönelik en çok atıf alan 20 yazar listelenmektedir. Buna göre ilk üç sırada olan yazarlar sırasıyla Siponen M.(n=18), Von Solms R. (n=32) Ve Çavuşoğlu M. (n=12) dir.



Şekil 5. En çok atıf alan yazarlar
(Most cited authors)

4.2. Siber Güvenlik ile İlgili Yayınların Kavramsal Yapısı (Conceptual Structure of Publications on Cyber Security)

Anahtar kelimeler, makalelerin özetini temsil eder bu nedenle anahtar kelimelerin çıkarılması ve sistematik olarak sınıflandırılması, araştırma alanının dinamiklerinin ve eğilimlerinin ortaya çıkarılması açısından önemlidir [34]. Şekil 6, siber güvenlik ve bilgi güvenliği konularındaki makalelerinin anahtar kelimelerinde en sık kullanılan kelime gruplarına yönelik kelime bulutunu göstermektedir. Kelimelerin sıklıklarına göre büyüklüklerinin belirlendiği bu kelime bulutu görseline göre; en sık kullanılan anahtar kelime "siber güvenlik", ikinci en sık kullanılan anahtar kelime "bilgi güvenliği" ve en yaygın üçüncü kelime "güvenlik" tir. Bu kelimeleri, "risk yönetimi", "bilgi güvenliği yönetimi", "risk değerlendirme", "bilgi güvenliği politikası" takip etmiştir. Bu görselden çıkan sonuçlara göre yayınların bilimsel faaliyet alanlarının hangi temalar üzerinde ağırlıklı olduğu görülmektedir.

Şekil 6. Kelime Bulutu
(Word Cloud)

Tablo 3'te siber güvenlik alanında yapılan yayınların trend olan araştırma konuları yıllara göre gösterilmektedir. Bu tabloda 2016-2021 yıllarına ait ve en fazla ön plana çıkan trend başlıklar sıralanmıştır. 2016 yılındaki en trend araştırma konuları sırasıyla risk yönetimi, risk değerlendirme, risk, bilgi güvenliği farkındalığı ve risk analizidir. 2017 yılında yayınlanan çalışmalarda trend konular; oyun teorisi, ağ güvenliği, kırılganlık, anomali teşhisi ve bilgi korumadır. 2018 yılındaki en popüler başlıklar bilgi güvenliği politikası, bilgi güvenliği kültürü, veri koruma, veri madenciliği ve tehditlerdir. 2019 yılında en trend başlıklar olarak akıllı şebekeler, farkındalık, uygunluk, siber uzay ve eğitim konularının ön plana çıktığı görülmektedir. 2020 yılında ise saldırı tespit, siber saldırılar, siber fiziksel sistemler, virüsler ve saldırı tespit sistemi gibi daha çok teknik araştırma konuları en trend başlık olarak karşımıza çıkmaktadır. 2021 yılına gelindiğinde oltalama, siber fiziksel güvenlik, analitik modeller, siber dayanıklılık ve organizasyonel kültür konularının popüler araştırma konuları olduğu görülmektedir. 2021 yılının en çok çalışılan araştırma konusu "oltalama", 2020 yılının "saldırı tespiti", 2019 yılının "akıllı şebekeler", 2018 yılının "bilgi güvenliği politikası", 2017 yılının "oyun teorisi", 2016 yılının ise "risk yönetimi" dir.

Tablo 3. Yıllara Göre Trend Konular
(Trending Topics by Years)

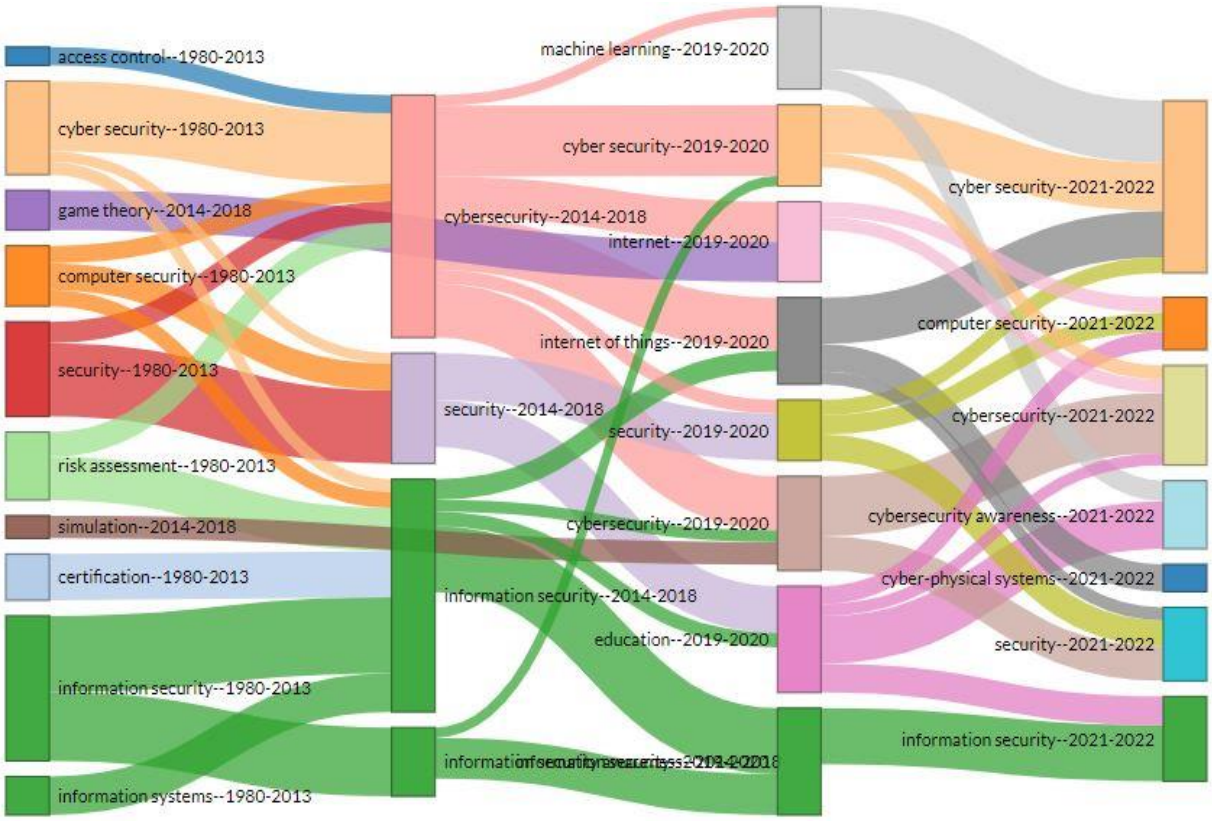
Yıl	Konu (Eng)	Konu (Tr)
2021	Phishing	Oltalama
	Cyber-Physical Security	Siber Fiziksel Güvenlik
	Analytical Models	Analitik Modeller
	Cyber Resilience	Siber Esneklik
	Organisational Culture	Kurumsal Kültür
2020	Intrusion Detection	Saldırı Tespiti
	Cyber-Attacks	Siber Saldırılar
	Cyber-Physical Systems	Siber Fiziksel Sistemler
	Malware	Kötü Amaçlı Yazılım
	Intrusion Detection System	Saldırı Tespit Sistemi
2019	Smart Grid	Akıllı Şebeke
	Awareness	Farkındalık
	Compliance	Uyum
	Cyberspace	Siber Uzay
	Education	Eğitim
2018	Information Security Policy	Bilgi Güvenliği Politikası
	Information Security Culture	Bilgi Güvenliği Kültürü
	Data Protection	Veri Koruma
	Data Mining	Ver Madenciliği
	Threats	Tehditler
2017	Game Theory	Oyun Teorisi
	Network Security	Ağ Güvenliği
	Vulnerability	Kırılganlık
	Anomaly Detection	Anomali tespiti
	Information Protection	Bilgi Koruma
2016	Risk Management	Risk Yönetimi
	Risk Assessment	Risk Değerlendirme
	Risk	Risk
	Information Security Awareness	Bilgi Güvenliği Farkındalığı
	Risk Analysis	Risk Analizi

4.3. Siber Güvenlik ile İlgili Yayınların Tematik Yapısı (Thematic Structure of Publications on Cyber Security)

Şekil 7 yıllara göre anahtar kelimelerin tematik gelişimini gösteren bir sankey diyaragramıdır. Siber güvenlik temalarının yıllara göre nasıl geliştiğini

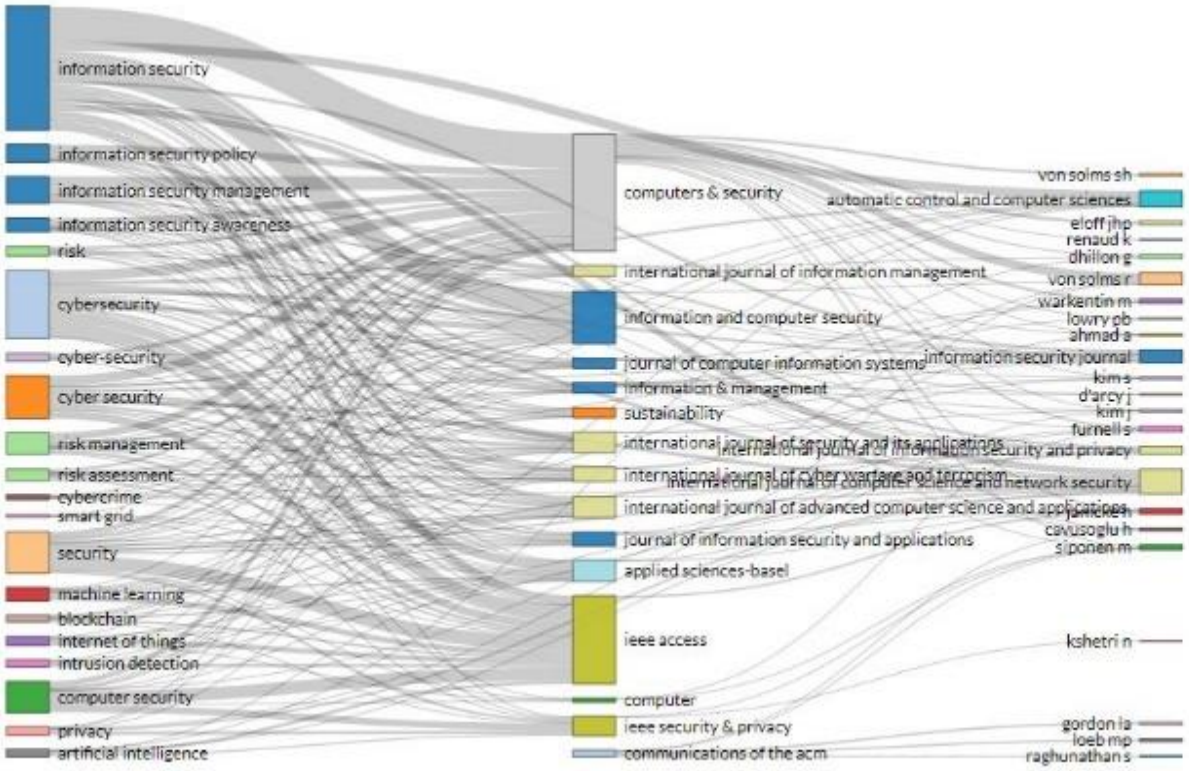
incelemek için sankey diyagramlarından yararlanılarak Tematik Evrim Haritası oluşturulmuştur. Sankey diyagramı ile tema kümelerinin oluşumu ve kümelerin zaman içinde birbirleriyle nasıl etkileşime geçtiği incelenir. Bu diyagramda tema kümeleri birbirleriyle boylamsal bir çerçeve içerisinde etkileşime girerler ve bu diyagram temaların ana evrimsel yollarını saptamaya olanak sağlar. Her bir düğüm noktası, en yüksek frekansa ve aynı zamanda uyumlu olduğu alt döneme karşılık gelen bir anahtar kelimeyle etiketlenen tema kümesini oluşturur. Düğümün boyutu ilgili tema içerisindeki anahtar kelimelerin sayısı ile doğru orantılıdır. Düğümler noktaları arasındaki akış, temaların evrimsel yönünü göstermektedir. Kenar genişliği birbirine bağlı iki temanın toplamı kadardır. Farklı dönemler boyunca gelişen bir grup tema, tematik bir küme olarak kabul edilebilir [20]. Siber güvenlik yayınlarında kullanılan anahtar kelimeler ile oluşturulan bu evrim haritası yayın sayılarına göre eşit bir şekilde dağılan dört döneme ayrılmıştır. Dört döneme yayılmasının sebebi zaman içerisindeki değişiklikleri net bir şekilde görebilmektir.

İlk dönem olan 1980-2013 arasında 10 tema varken bu temalar son dönem olan 2021-2022 döneminde 7 tema altında toplanmıştır. İlk dönemde bilgi güvenliği ağırlıklı tema iken son dönemde siber güvenlik teması ağırlıklıdır. İlk dönemde hiç bulunmayan siber güvenlik farkındalığı ve siber fiziksel sistemler temaları son dönemde etkin tema olmuştur.



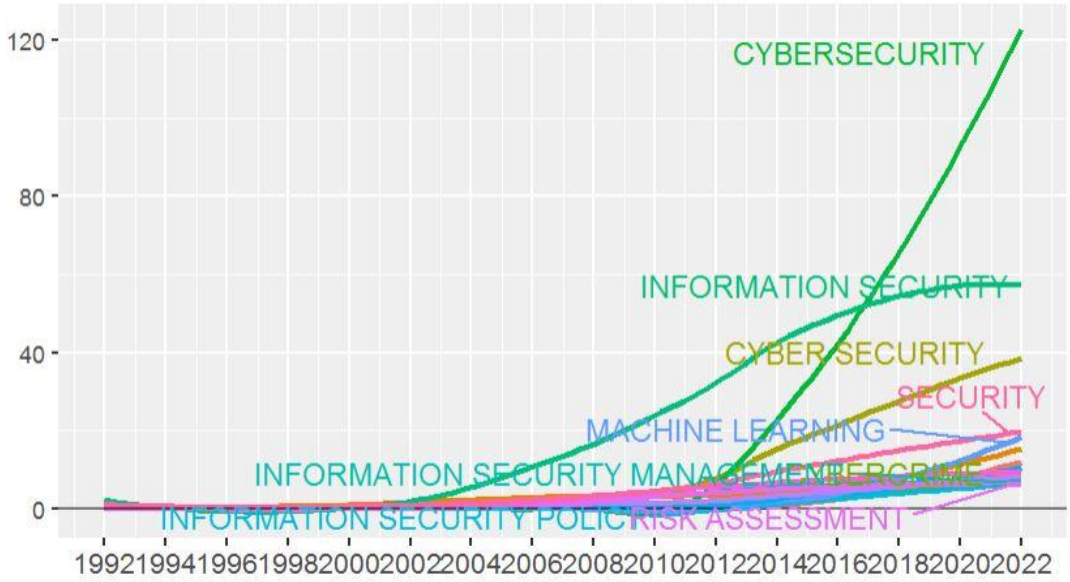
Şekil 7. Tematik Evrim Haritası(Sankey Diyagramı)
(Thematic Evolution Map (Sankey Diagram))

Anahtar kelimeler, yazarlar ve dergiler arasındaki ilişki üç alan grafiği Şekil 8'de gösterilmiştir. Buna göre; siber güvenlik alanında yapılan çalışmaların en çok yayımlandığı dergiler, bu dergilere en çok katkı sağlayan yazarlar ve yazarların en çok kullandığı anahtar kelime temaları gösterilmektedir. Grafikte yer alan düğümlerin boyutunun büyüklüğü veya küçüklüğü bu öğelerle ilişkili yayın sayısıyla orantılıdır. Üç alan grafiğinin solunda yazalar anahtar kelimeleri yer almakta ve bu alanda 20 farklı anahtar kelime listelenmektedir. Buna göre en çok kullanılan anahtar kelimelerin bilgi güvenliği, bilgi güvenliği politikası, bilgi güvenliği yönetimi, bilgi güvenliği farkındalığı, bilgisayar güvenliği olduğu görülmektedir. Grafiğin ortasında çalışmaların en çok yayımlandığı yayınladığı dergiler yer almaktadır. Buna göre siber güvenlik alanında en çok yayım yapılan dergilerin "computers & security", "ieee access", "information and computer security" olduğu göze çarpmaktadır. Grafiğin sağ tarafında ise bu alanda yayın yapan yazarlar yer almaktadır. Gri çizgiler ise düğümler arasındaki ilişkileri göstermektedir.



Şekil 8. Anahtar Kelimeler, Dergiler ve Yazarlar Arasındaki İlişkinin Üç Alan Grafiği
(Three Area Graphs of Relationship Between Keywords, Journals, and Authors)

Yazar anahtar kelime analizine dayalı yıllara göre araştırma eğilimleri Şekil 9'da gösterilmektedir. Bu grafiğe göre siber güvenlik anahtar kelimesi giderek artan bir kullanımı varken bilgi güvenliği anahtar kelimesinin yavaş ve 2020 yılı itibari daha dengeli bir düzeyde ilerleme göstermektedir. Bilgi güvenliği yönetimi, bilgi güvenliği politikası anahtar kelimelerinin ise 2000 yıllar öncesinde daha az çalışılmış iken 2000 yıllar sonrasında ivme kazandığı ve bu anahtar kelimelerin yayınlarda kullanım sıklığının arttığı Şekil 9' da görülmektedir.



Şekil 9. Yıllara Göre Anahtar Kelimelerin Eğim Analizi
(Slope Analysis of Keywords by Year)

Yazar anahtar kelimelerinin birlikte kullanımını inceleyebilmek için eşdizimlilik ağına ait grafik Şekil 10'da sunulmaktadır. Eşdizimlilik ağı sık sık birlikte kullanılan anahtar kelimeleri bir küme içinde gruplandıran bir analizdir. Alanın tematik yapısını ortaya koyan bu grafikte her bir renk bir kümeyi temsil

etmektedir. İlk küme olan "information security" teması içerisinde "bilgi güvenliği yönetimi, bilgi güvenliği farkındalığı, güvenlik yönetimi, bilgi güvenliği kültürü, bilgi güvenliği politikası, risk yönetimi, risk değerlendirme, risk analizi" gibi kavramlar ana tema ile yoğun bir ilişki içerisindedir. Mavi renk ile küme grubunun temel odak noktası "cyber security" başlığıdır. Bu temada "büyük veri, siber suçlar, akıllı şebekeler, nesnelerin interneti, saldırı tespiti, makine öğrenmesi, derin öğrenme, yapay zeka, bulut bilişim, siber uzay, blok zincir" kavramları yer almaktadır. Üçüncü küme ise kırmızı renk ile belirtilen "security" kümesidir. Bu başlık altında "kriptografi, bilgisayar suçları, öğrenme, eğitim, gizlilik, savunmasızlık, ağ güvenliği, bilgisayar güvenliği, oyun teorisi, insan faktörleri, risk" kavramları ile ilişkiler yer almaktadır.

Şekil 10. Anahtar Kelimeler Göre Eşdizimlilik Ağı
(Collocation Network by Keywords)

5. TARTIŞMA VE SONUÇ (DISCUSSION and CONCLUSION)

Bu çalışmanın amacı, siber güvenlik ile ilgili alan dinamiklerini ve son araştırma eğilimlerini ortaya koymaktır. Bu amaç doğrultusunda alanın performans göstergeleri, kavramsal ve tematik yapısı incelemek ve anlamak için bibliyometrik analiz yapılmıştır. Araştırmanın amacı doğrultusunda "Siber güvenlik ile ilgili yayınların performans göstergeleri nelerdir?", "Siber güvenlik ile ilgili yayınların kavramsal yapısı nasıldır ve ön plana çıkan unsurlar nelerdir?", "Siber güvenlik ile ilgili yayınların tematik gelişim haritasında ön plana çıkan unsurlar nelerdir? "araştırma sorularına cevap aranmıştır.

Araştırma Sorusu 1: Siber güvenlik alanı ile ilgili yayınların performans göstergeleri nelerdir? (En çok katkı sunan yayınlar, dergiler, ülkeler, atıf alan yazarlar)

Siber güvenlik ilgili literatürün yazarlığı ve küresel dağılımı incelediğinde, ABD'nin atıf açısından en fazla yayına ve etkiye sahip olduğunu görülürken, gelişmekte olan ülkelerin araştırma atıf sayısının az olduğu görülmüştür. Dolayısıyla gelişmekte olan ülkelerde araştırma sayısının arttırılması ve araştırmacıların bu konuya yönelmesine alanın gelişmesi için ihtiyaç duyulmaktadır. Bulgular, bu konudaki literatürün 1980 yılında başladığını ve 2021'de 688 yayınla zirveye ulaştığını, söz konusu bu yıllar arasında toplam 4252 çalışmanın yayınladığını göstermektedir. Buna göre, bu konudaki yayınlar 2015 yılı itibariyle ivme kazanmıştır (Şekil 3). Son beş yılda toplam yayın sayısının yarısından fazlasının yayımlandığı gözlenmektedir. Analizler neticesinde siber güvenlik ile ilgili literatürün küresel dağılımının sınırlı kaldığı görülmüştür. Özellikle ABD, Çin gibi gelişmiş ülkelerdeki yayın sayısı gelişmekte olan ülkelere kıyasla yüksek seyretmiştir [17], [19]. Siber güvenlik ülke sınırlarını aşan küresel bir fenomen olduğu için bireylerin siber uzay ortamında güvenliğinin nasıl sağlanacağı konusunda ortak iş birlikli araştırmalar yürütülmesi alanın gelişimi adına önemli olacaktır.

Araştırma Sorusu 2: Siber güvenlik alanı ile ilgili yayınların kavramsal yapısı nasıldır ve ön plana çıkan unsurlar nelerdir?

Alanın kavramsal yapısı yıllara göre incelediğinde her yıl ayrı çalışma temalarının ortaya çıktığı görülmektedir. Anahtar kelime analizine göre yazarlar tarafından araştırılan en çok kullanılan anahtar kelimeler yıllara göre kategorileştirilmiştir (Tablo 3). 2016 yılında yayınlanan araştırmalarda en çok tekrar eden anahtar kelimeler sırasıyla risk yönetimi, risk değerlendirme, risk, bilgi güvenliği farkındalığı ve risk analizidir. 2017 yılında yayınlanan araştırmalarda en çok tekrar eden anahtar kelimeler; oyun teorisi, ağ güvenliği, kırılganlık, anomali teşhisi ve bilgi korumadır. 2018 yılındaki en popüler başlıklar bilgi güvenliği politikası, bilgi güvenliği kültürü, veri koruma, veri madenciliği ve tehditlerdir. 2019 yılında yayınlanan araştırmalarda akıllı şebekeler, farkındalık, uygunluk, siber uzay ve eğitim konularının ön plana çıktığı görülmektedir. 2020 yılında ise saldırı tespit, siber saldırılar, siber fiziksel sistemler, virüsler ve saldırı tespit sistemi gibi daha çok teknik araştırma konuları en trend başlık olarak karşımıza çıkmaktadır. 2021 yılında oltalama, siber fiziksel güvenlik, analitik modeller, siber dayanıklılık ve organizasyonel kültür konularının popüler araştırma konuları olduğu görülmektedir. 2021 yılının en çok çalışılan araştırma konusu "oltalama", 2020 yılının "saldırı tespiti", 2019 yılının "akıllı şebekeler", 2018 yılının "bilgi güvenliği politikası", 2017 yılının "oyun teorisi", 2016 yılının ise "risk yönetimi" olmuştur. Tüm bu anahtar kelimeler siber güvenlik ile bağlantılıdır. Bu anahtar kelimelerden "saldırı tespiti" ve "akıllı şebekeler" önceki çalışmaların bulguları ile örtüşmektedir [18], [20]. Bu çalışma ortaya çıkardığı diğer anahtar kelimeler ile mevcut literatürden ayrışmakta ve bu yönüyle alana önemli katkı sunmaktadır.

Araştırma Sorusu 3: Siber güvenlik alanı ile ilgili yayınların tematik gelişim haritasında ön plana çıkan unsurlar nelerdir?

Siber güvenlik alanının tematik gelişim haritası incelediğinde 1980-2013 arasında 10 tema varken bu temalar son dönem olan 2021-2022 döneminde 7 tema altında toplanmıştır (Şekil 7). İlk dönemde bilgi güvenliği ağırlıklı tema iken son dönemde siber güvenlik teması ağırlıklıdır. İlk dönemde hiç bulunmayan siber güvenlik farkındalığı ve siber fiziksel sistemler temaları son dönemde etkin tema olmuştur. Önceki çalışmalar siber güvenlikle ilgili makalelerin çoğunun teknolojiye odaklandığını, alanın sosyal boyutunu temsil eden insani ve organizasyonel yönlerin yeterince incelenmediğini ortaya çıkarmıştır [35]. Bu araştırma bu bulguları desteklemekte olup son yıllarda araştırmacıların teknik konulardan artık davranışsal sosyal konulara kaydığını, günümüzde artık siber güvenliğin sosyal boyutunun öne çıktığı yapılan analizler neticesinde görülmektedir. Siber güvenlik olaylarının büyük bir çoğunluğunun sebebi insan faktörüdür. Bu nedenle gelecek çalışmaların siber güvenliğin insani ve organizasyonel yönlerinin araştırılması önerilmektedir.

Alanın tematik yapısını ortaya koyan eş dizimlilik ağı incelediğinde **"information security"** teması içerisinde "bilgi güvenliği yönetimi, bilgi güvenliği farkındalığı, güvenlik yönetimi, bilgi güvenliği kültürü, bilgi güvenliği politikası, risk yönetimi, risk değerlendirme, risk analizi" gibi kavramlar ana tema ile yoğun bir ilişki içerisindedir. Diğer bir tema ise **"cyber security"** başlığıdır. Bu temada "büyük veri, siber suçlar, akıllı şebekeler, nesnelerin interneti, saldırı tespiti, makine öğrenmesi, derin öğrenme, yapay zeka, bulut bilişim, siber uzay, blokzincir" kavramları yer almaktadır. Üçüncü tema ise **"security"** kümesidir. Bu başlık altında "kriptografi, bilgisayar suçları, öğrenme, eğitim, gizlilik, savunmasızlık, ağ güvenliği, bilgisayar güvenliği, oyun teorisi, insan faktörleri, risk" kavramları ile ilişkiler yer almaktadır. Sonuç olarak, bu grafikte araştırma alanıyla ilgili en önemli kavramlar ve birbiri ile yakın bir şekilde ilişkili olan kavramlar kümelenmişlerdir (Şekil 10). Bu bulgulardan hareketle araştırma alanının temel yapıtaşları görülebilmektedir.

5.1. Teorik ve Pratik Katkılar (Theoretical and Practical Implications)

Bu çalışma, siber güvenlik konusunda teorik ve pratik olarak alana katkı verecektir. İlk olarak araştırmanın kullandığı arama stratejisi, yıl kapsamı ve makale sayısı açısından mevcut çalışmalardan ayrışarak literatüre katkı sağlayacaktır. Araştırma, Türkiye'de siber güvenlik ve bilgi güvenliği alanındaki literatürün çeşitli bibliyometrik indekslerini analiz eden ilk araştırmalardan biri olarak alana katkı sunacaktır. Pratikte ise, araştırmacıların ve bilim uzmanlarının siber güvenlik alanına yönelik farkındalık düzeyini artırmak ve bu alandaki çalışmalara yol gösterici katkısı olacağı düşünülmektedir. Yeni teknolojiler ortaya çıktıkça siber saldırıların boyutu ve yöntemi değişmektedir. Bu nedenle siber güvenlik araştırmalarının yeni teknolojiler bağlamında (örn. Yapay zeka, Metaverse) inceleyen çalışmalara daha çok ihtiyaç duyulmaktadır.

5.2. Sınırlılıklar ve Gelecek Araştırmalar İçin Öneriler (Limitations of the Study and Directions for Future Studies)

Bu araştırmada her araştırmada olduğu gibi bazı sınırlılıklara sahiptir. Gelecek araştırmalar için bu sınırlılıklar birer avantaj haline dönüştürülerek alana daha derin katkılar sağlanabilir. İlk olarak kullanılan veri tabanı nedeniyle bazı sınırlılıklar vardır. Bu araştırmada Web of Science veri tabanında veriler elde edilmiştir. Web of Science, bilimsel dergiler, kitaplar ve konferans bildirileri de dahil olmak üzere hakemli literatür için en büyük özet ve alıntı arşivi olmasına rağmen tüm dergileri ve yayınları arşivleyememektedir. Bu nedenle bazı dergilerdeki yayınlar araştırma kapsamı dışında kalmış olabilir. Gelecek araştırmalar, siber güvenlik konusunda yayınlanmış çalışmalar hakkında tam ve ayrıntılı bulgular elde etmek için ek veri tabanları kullanılarak yeni çalışmalar yapılabilir. Çeşitli veri tabanlarından elde edilen bulgular arasındaki paralellikleri ve tutarsızlıkları tespit etmek için

genellikle karşılaştırmalı araştırmalar yapılması önerilmektedir. Ek olarak, gelecekteki araştırmalar, zengin bilgi elde etmek için görüşmeler, grup tartışmaları, anketler veya diğer yaklaşımlar gibi bir dizi araştırma tekniğini kullanarak alanın detaylı incelemesini yapabilirler. İkincisi, bu makalede yayınların başlıklarına, özetlerine ve anahtar sözcüklerine dayalı analizler yapılmıştır. Üçüncüsü, yıllara göre veri tabanı sürekli olarak değiştiğinden, kümülatif yayın sayısı ve toplanan diğer ayrıntılar yalnızca belirli zaman aralığı dahilinde incelenmiştir. Veri toplama aşaması Ağustos 2022 tarihinde bitirildiğinden gelecekteki araştırmalar zaman aralığını uzatarak, alanın gelişiminin geniş zaman diliminde ele alınması tavsiye edilmektedir. Sonuç olarak, bu çalışmada siber güvenlik ve bilgi güvenliği konusunda gelecekteki araştırmalar için temel oluşturmak amaçlanmıştır.

KAYNAKLAR (REFERENCES)

[1] A. Pawlicka, M. Choraś, and M. Pawlicki, "Cyberspace threats: Not only hackers and criminals. Raising the awareness of selected unusual cyberspace actors - Cybersecurity researchers' perspective", **ACM International Conference Proceeding Series.** 2020.

[2] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade", IEEE Access, 8, 222310–222354, 2020.

[3] V. Aliusta and R. Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Cilt:4, 2,35–42, 2018.

[4] Statista, "Global internet penetration rate by region 2023 | Statista," 2022. https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/ 20.03. 2023.

[5] Statista, "Devices used to access the internet 2022 | Statista," 2022. https://www.statista.com/statistics/1289755/internet-access-by-device-worldwide/ 20.03, 2023.

[6] T. Aslan, B. Aktaş, and A. Akbıyık, "Kullanıcıların Bilgisayar Güvenliği Davranışını İnceleme: Siber Hijyen", **7. Uluslararası Yönetim Bilişim Sistemleri Konferansı,** Bakırçay Üniversitesi, İzmir, 3–10, 9-11 Aralık 2020.

[7] F. A. Loan, B. Bisma, and N. Nahida, "Global Research Productivity in Cybersecurity: A Scientometric Study", Global Knowledge, Memory Communication, 71, 4–5, 342–354, 2022.

[8] İ. Tuğal, C. Almaz, and M. Sevi, "Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri", *Bilişim Teknolojileri Dergisi*, 14, 3, 229–238, 2021.

[9] B. von Solms and R. von Solms, "Cybersecurity And İnformation Security – What Goes Where?", Information Computer Security, 26, 2–9, 2018.

[10] B. Elango, S. Matilda, and J. Jeyasankari, "Redefining Search Terms for Cybersecurity: A Bibliometric Perspective", SSRN Electron. J., 2020.

[11] Kaspersky, "What is Cyber Security? | Definition, Types, and User Protection | Kaspersky," Www.Kaspersky.Co.Uk. p. Home/Resource Centre/Definitions, 2019. https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security. 21.02. 2022.

[12] A. Klimburg, **"Natıonal Cyber Securıty Framework Manual"**, 2012.

[13] F. Wamala, **"ITU National Cybersecurity Strategy Guide"**, 2011.

[14] R. Solms and J. Niekerk, "From İnformation Security to CyberSecurity", Computer Security, 38,97–102, 2013.

[15] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis, and S. Madnick, "Health Care and Cybersecurity: Bibliometric Analysis of the Literature", *Journal Medical Internet Research* 21, 2, 12644, 2019.

[16] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A Systematic Literature Review of Blockchain Cyber Security", Digital Communication Networks, 6, 2, 147–156, 2020.

[17] N. Rahim, "Bibliometric Analysis of Cyber Threat and Cyber Attack Literature: Exploring the Higher Education Context", Cybersecurity Threat. with New Perspect. 1–17, 2021.

[18] B. Elango, S. Matilda, M. Martina Jose Mary, and M. Arul Pugazhendhi, "Mapping the Cybersecurity Research: A Scientometric Analysis of Indian Publications" , 4, 1-17 2022.

[19] F. A. Loan, B. Bisma, and N. Nahida, "Global research productivity in cybersecurity: a scientometric study", Global Knowledge, Memory Communication, 71, 4–5, 342–354, 2022.

[20] D. Sharma, R. Mittal, R. Sekhar, P. Shah, and M. Renz, "A Bibliometric Analysis of Cyber Security and Cyber Forensics Research", Results in Control and Optimization, 10, 100204, 2023.

[21] H. Ying et al., "A Bibliometric Analysis of Research on Heart Failure Comorbid With Depression from 2002 to 2021", Heliyon, 13054, 2023.

[22] H. Xie, Y. Zhang, Z. Wu, and T. Lv, "A Bibliometric Analysis on Land Degradation: Current Status, Development, and Future Directions", Land, 9, 1, 2020.

[23] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", IEEE Communication Survey Tutorials, 18, 2, 1153–1176, 2016.

[24] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", MIS Quarterly, 34, 3, 523–548, 2010.

[25] W. Wang and Z. Lu, "Cyber Security in the Smart Grid: Survey and Challenges", Computer Networks, 57, 5, 1344–1371, 2013.

[26] B. A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors : an Empirical Study", MIS Quarterly, 34, 3, 549–566, 2010.

[27] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions. Information Forensics Securutiy, 1, 2, 125–143, 2006.

[28] P. Puhakainen and M. Siponen, "Improving Employees' Compliance Through İnformation Systems Security Training: An Action Research Study", MIS Quarterly. Management Information Systems, 34, 4, 757–778, 2010.

[29] T. Herath and H. R. Rao, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness", Decision Support Systems, 47, 2, 154–165, 2009.

[30] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications", IEEE Communications Surveys and Tutorials, 14, 4, 998–1010, 2012.

[31] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future Directions for Behavioral Information Security Research", Computer Security, 32, 90–101, 2013.

[32] P. Ifinedo, "Understanding Information Systems Security Policy Compliance: An Integration of The Theory of Planned Behavior and The Protection Motivation Theory", Computer Security, 31, 1, 83–95, 2012.

[33] D. Fiala and G. Tutoky, "Computer Science Papers in Web of Science: A Bibliometric Analysis", Publications, 5, 4, 2017.

[34] X. Lyu, W. Peng, W. Yu, Z. Xin, S. Niu, and Y. Qu, "Sustainable Intensification to Coordinate agricultural Efficiency And Environmental Protection: A Systematic Review Based on Metrological Visualization", *Journal Land Use Science*, 16, 3, 313–338, 2021.

[35] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis, and S. Madnick, "Health Care and Cybersecurity: Bibliometric Analysis of The Literature", *Journal Medical Internet Research*, 21, 2, 1–18, 2019.