Applied Scientometric Studies
Volume 2, Issue 1, 2025

Scientometric Analysis of Cyber Resilience in Financial and Banking Systems: Trends, Gaps, and Future Perspectives

SeyyedAli Doorafshan[1], and **Mahsa Pishdar**[2]

1. PhD Candidate in Industrial Management, University of Tehran, Tehran, Iran; Email sa.doorafshan@ut.ac.ir
2. Assistant Professor, College of Farabi, University of Tehran, Qom, Iran; Email mahsa.pishdar@ut.ac.ir

Article Info

Article type:
Research

Article history:
Received: 2025/06/11
Accepted: 2025/07/27
Available online: 2025/08/11

Keywords:
Cyber resilience, Cybersecurity, Finance, Banking, FinTech, Scientometrics, Scopus.

ABSTRACT

Purpose: Cyber resilience in financial and banking systems has emerged as a strategic necessity to counter technological threats and systemic crises. The growing sophistication of cyberattacks, the rapid expansion of digital financial services, and the increasing interdependence of financial infrastructures on networked technologies have elevated cyber resilience from a purely technical issue to a central pillar of financial stability. This study aims to map the scientific landscape of research on cyber resilience in financial and banking systems by identifying research trends, key contributors, thematic clusters, and knowledge gaps over the period 2018–2025.

Methodology: The study adopts a bibliometric approach to analyze the structure and evolution of research in this domain. Data was extracted from the Scopus database using a comprehensive Boolean search strategy that incorporated combinations of terms related to *Cyber Resilience*, *Banking*, and *Financial Systems*. The time frame was limited to 2018–2025 and the language to English. The raw data were cleaned and standardized using Open Refine to correct inconsistencies in author names, institutions, and keywords. Subsequently, the data were processed for network and visualization analyses using VOS viewer, while complementary descriptive and statistical analyses were conducted in Python with the *Pandas*, *NumPy*, and *Matplotlib* libraries. This methodological integration provided a comprehensive quantitative overview of the field across temporal, geographical, and conceptual dimensions.

Findings: The bibliometric distribution reveals a consistent upward trend in scientific output related to cyber resilience in financial systems, with the highest growth observed in 2023 and 2024. This surge reflects global attention to cybersecurity challenges arising from the expansion of fintech and digital finance. The United States, China, the United Kingdom, and Germany emerged as the dominant knowledge producers, while countries such as India and Australia play secondary but growing roles. The global collaboration network remains highly centralized around the U.S.–China axis, with limited participation from developing nations.

Conceptual and co-word analyses identified seven major thematic clusters structuring the literature:

Light Blue Cluster: Technical and defensive aspects (cybersecurity, network security, data protection).

Green Cluster: Cyber resilience and risk management, linking technical and financial dimensions.

Red Cluster: Emerging technologies (artificial intelligence, fintech, cyber fraud).

Black Cluster: Independent focus on risk assessment frameworks.

Purple Cluster: Policy, regulation, and socio-organizational resilience.

Turquoise Cluster: Critical infrastructure, smart cities, and cyber autonomy.

Yellow Cluster: Emerging topics such as sustainability, blockchain, e-commerce, and intrusion detection.

This clustering demonstrates a clear conceptual transition from a purely technical and defensive orientation toward a multidimensional, interdisciplinary, and system-level perspective where resilience, innovation, and sustainability converge.

Conclusion: The bibliometric evidence suggests that the field of cyber resilience in financial and banking systems is approaching conceptual maturity, yet significant research gaps persist. These include the scarcity of empirical studies within real-world financial institutions, the lack of integrated frameworks combining technical, institutional, and economic dimensions, and limited international and interdisciplinary collaborations. To advance this domain, financial institutions must shift from a reactive stance to systemic resilience management, leveraging technologies such as Artificial Intelligence (AI), Blockchain, and Decentralized Finance (DeFi) for continuous

monitoring, enhanced transparency, and improved responsiveness. Overall, this study highlights the pivotal role of cyber resilience in sustaining the integrity and stability of modern financial ecosystems. The integration of bibliometric and qualitative approaches, expansion of data sources, and development of standardized resilience assessment metrics are recommended pathways for future research.

Cite this article: Doorafshan, SeyyedAli; Pishdar, Mahsa (2025). Scientometric Analysis of Cyber Resilience in Financial and Banking Systems: Trends, Gaps, and Future Perspectives, *Applied Scientometric Studies*, 2(2), 70 - 92. https://doi.org/10.22091/apss.2026.14202.1068

Publisher: University of Qom.
DOI: http//doi.org/10.22091/apss.2026.14202.1068

مطالعات کاربردی علم‌سنجی
دوره ۲، شماره ۱، ۱۴۰۴

تحلیل علم‌سنجی تاب‌آوری سایبری در نظام‌های مالی و بانکی: روندها، شکاف‌ها، و چشم‌انداز آینده

سیدعلی درافشان[۱]، و مهسا پیشدار[۲]

۱. گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشکدگان فارابی دانشگاه تهران، قم. رایانامه: sa.doorafshan@ut.ac.ir
۲. گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشکدگان فارابی دانشگاه تهران، قم (نویسنده مسئول). رایانامه: mahsa.pishdar@ut.ac.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی.

تاریخچه مقاله:
تاریخ دریافت: ۱۴۰۴/۰۳/۲۱
تاریخ پذیرش: ۱۴۰۴/۰۵/۰۵
تاریخ انتشار: ۱۴۰۴/۰۵/۲۰

کلیدواژه‌ها:
تاب آوری سایبری، امنیت سایبری، مالی ،بانکی، فین‌تک، علم‌سنجی، اسکوپوس.

چکیده

هدف: تاب‌آوری سایبری نظام‌های مالی و بانکی در سال‌های اخیر به ضرورتی راهبردی برای مقابله با تهدیدات فناورانه و بحران‌های سیستمایک تبدیل شده است. افزایش حملات پیچیده، گسترش خدمات مالی دیجیتال، و وابستگی شدید زیرساخت‌های مالی به فناوری‌های شبکه‌ای، این مفهوم را از سطحی فنی به مؤلفه‌ای حیاتی در ثبات و پایداری اقتصادی ارتقاء داده است. پژوهش حاضر با هدف ترسیم نقشهٔ دانش و شناسایی روندهای علمی، بازیگران کلیدی، خوشه‌های موضوعی، و شکاف‌های پژوهشی، به تحلیل علم‌سنجی تاب‌آوری سایبری در نظام‌های مالی و بانکی در بازه زمانی ۲۰۱۸ تا ۲۰۲۵ پرداخته است.

روش‌شناسی: روش این پژوهش مبتنی‌بر رویکرد علم‌سنجی است. داده‌ها از پایگاه اسکوپوس استخراج شده و پرس‌وجوی جست‌وجو با هدف پوشش جامع ترکیبات واژگانی مرتبط با مفاهیم Cyber Resilience، Banking و Financial Systemsطراحی شد. محدودیت زمانی ۲۰۱۸ تا ۲۰۲۵ و زبان انگلیسی اعمال شد. داده‌های خام با اُپن ریفاین پاک‌سازی و یکپارچه شدند تا خطاهای ناشی از ناهمگونی اسامی نویسندگان و مؤسسات حذف شود. سپس داده‌ها برای تحلیل شبکه‌ای و مصوُرسازی در وی.اُ.اس ویور و تحلیل‌های آماری تکمیلی با پایتون و کتابخانه‌های پانداس[۱]، نامپای[۲] و متپلات‌لیب[۳] پردازش شدند. ترکیب این ابزارها تصویری کمّی و جامع از وضعیت علم‌سنجی، ساختار همکاری‌های علمی، و مفاهیم محوری حوزه ارائه کرده است.

یافته‌ها: یافته‌ها نشان می‌دهد تولید دانش در این حوزه طی سال‌های اخیر روندی صعودی و شتاب‌گیرنده داشته و بیشترین رشد در سال‌های ۲۰۲۳ و ۲۰۲۴ مشاهده می‌شود؛ دوره‌ای که هم‌زمان با گسترش فین‌تک‌ها و افزایش تهدیدات سایبری، توجه جهانی به امنیت مالی شدت یافته است. ایالات متحده، چین، انگلستان، و آلمان بیشترین سهم را در تولید دانش و همکاری علمی دارند و هسته‌های اصلی شبکهٔ جهانی به شمار می‌روند. با این حال، مشارکت کشورهای درحال‌توسعه هنوز محدود و شبکهٔ جهانی همکاری‌ها تمرکزگرا است. تحلیل هم‌واژگانی نشان داد که ادبیات علمی تاب‌آوری سایبری نظام‌های مالی در قالب هفت خوشهٔ مفهومی سازمان‌یافته است: خوشهٔ آبی روشن با محوریت امنیت سایبری، امنیت شبکه و حفاظت از داده‌ها (رویکرد فنی)، خوشهٔ سبز مرتبط با تاب‌آوری و مدیریت ریسک (پیوند فنی_مالی)، خوشهٔ قرمز شامل مفاهیم هوش مصنوعی، فین‌تک و تقلب سایبری (فناوری‌های نوین مالی)، خوشهٔ سیاه با تمرکز مستقل بر ارزیابی ریسک، خوشهٔ بنفش درباره سیاست‌گذاری و مقررات سایبری. خوشهٔ فیروزه‌ای شامل زیرساخت‌های حیاتی، شهر هوشمند، و خودمختاری سایبری. خوشهٔ زرد مرتبط با موضوعات نوظهور نظیر پایداری، بلاکچین، تجارت الکترونیک و تشخیص نفوذ.این ساختار نشان می‌دهد که تمرکز پژوهش‌ها از ابعاد تنها فنی به دیدگاهی چندسطحی و میان‌رشته‌ای تحوّل یافته است، جایی که پایداری و تاب‌آوری مالی با فناوری‌های نوین درهم تنیده‌اند.

نتیجه‌گیری: نتایج کلی نشان می‌دهد که حوزهٔ تاب‌آوری سایبری در نظام‌های مالی به‌سوی بلوغ مفهومی در حرکت است، اما هنوز شکاف‌هایی برجسته باقی مانده‌اند. مهمترین آن‌ها عبارت‌اند از: نبودِ مطالعات تجربی در محیط‌های

1. Pandas
2. NumPy
3. Matplotlib

بانکی واقعی، نبودِ چارچوب‌های جامع ارزیابی ریسک که ابعاد فنی، نهادی، و اقتصادی را تلفیق کنند، و محدودیت همکاری‌های میان‌رشته‌ای و بین‌المللی. برای گذار از این وضعیت، نهادهای مالی باید از رویکرد واکنشی به‌سمت مدیریت تاب‌آوری سیستمی حرکت کنند و از فناوری‌های هوش مصنوعی، بلاکچین، و امور مالی غیرمتمرکز برای پایش مداوم تهدیدات، ارتقاء شفافیت، و تقویت پاسخ‌گویی استفاده نمایند. به‌طور کلی، پژوهش حاضر نشان می‌دهد تاب‌آوری سایبری اکنون در تعامل با فناوری‌های نوظهور، در پایداری نظام‌های مالی نقش بنیادینی ایفا می‌کند. استفادهٔ ترکیبی از روش‌های علم‌سنجی و تحلیل‌های کیفی، گسترش پایگاه‌های داده، و تدوین شاخص‌های معتبر سنجش عملکرد تاب‌آوری، مسیر آینده این حوزه را شکل خواهد داد.

استناد: درافشان، سیدعلی؛ پیشدار، مهسا (۱۴۰۴). تحلیل علم‌سنجی تاب‌آوری سایبری در نظام‌های مالی و بانکی: روندها، شکاف‌ها، و چشم‌انداز آینده. *مطالعات کاربردی علم‌سنجی*، ۲ (۲)، ۹۲-۷۰. https://doi.org/10.22091/apss.2026.14202.1068

ناشر: دانشگاه قم.

۱. مقدمه و بیان مسئله

در دهه‌های اخیر، تحلیل علم‌سنجی به ابزاری بنیادین برای نقشه‌برداری نظام‌مند از تکامل علمی، شناسایی الگوهای همکاری، و جهت‌گیری‌های موضوعی پژوهش‌ها تبدیل شده و بنیانی برای پژوهش‌های آکادمیک و توسعهٔ سیاست‌گذاری فراهم کرده است (شکفته و همکاران، ۲۰۱۶؛ لوپز-پرناس و دیگران، ۲۰۲۳)[1]. این حوزه که ریشه در تلاش‌های اولیه برای ترسیم ساختار و رشد علم دارد، از شمارش تنها انتشارات و استنادها فراتر رفته و به‌سمت ارزیابی‌های چندبُعدی حرکت کرده است؛ ارزیابی‌هایی که شاخص‌های اثر اجتماعی، همکاری‌های بین‌المللی، و نوآوری‌های علمی را نیز دربرمی‌گیرند. نظریه‌های کلیدی مانند قانون لوتکا (توزیع تولید علمی) و قانون بردفورد (پراکندگی مجلات) همچنان چارچوب نظری این حوزه را شکل می‌دهند. هم‌زمان، روش‌های علم‌سنجی از تحلیل‌های سادهٔ استنادی به مدل‌های پیچیده‌تر مبتنی‌بر یادگیری ماشین و تحلیل شبکه‌های اجتماعی تکامل یافته‌اند و ابزارهایی مانند وبآوساینس[2]، اسکوپوس[3]، و گوگل اسکالر[4] برای چنین تحلیل‌هایی داده‌های گسترده و به‌روز فراهم می‌کنند. درحالی‌که نرم‌افزارهایی نظیر وی.اُ.اس ویوِر[5]، یوسی‌نت[6]، پاژک[7]، بایب‌اکسل[8]، ، ، و غیره امکان تجسم و نقشه‌برداری خوشه‌های علمی و ساختارهای شبکه‌ای را فراهم می‌آورند (یائو و دیگران، ۲۰۲۵؛ جسورا، ۲۰۲۴، ۲۰۲۵)[9]. این تحوُل روش‌ها و ابزارها باعث شده است علم سنجی از یک ابزار کمّی ساده به یک رویکرد چندلایه و قدرتمند تبدیل شود که مسیرهای شکل‌گیری دانش و شبکه‌های تأثیرگذاری علمی را آشکار و دینامیک‌های پژوهش در رشته‌های گوناگون را ترسیم می‌کند؛ به همین دلیل، سیاست‌گذاران، نهادهای تأمین مالی، و مؤسسات دانشگاهی به‌طور فزاینده‌ای به شاخص‌های علم‌سنجی برای تصمیم‌گیری راهبردی، تخصیص منابع، و شناسایی روندهای نوظهور متُکی هستند (باخمت،۲۰۲۲؛ پوئنته و دیگران،۲۰۲۴)[10].

در این بستر، تاب‌آوری سایبری یکی از حوزه‌های نوظهور است که در پیوند امنیت و اقتصاد دیجیتال اهمیت فزاینده‌ای یافته است. تحوّل دیجیتال در سیستم‌های مالی و بانکی، ریسک‌های سایبری را از یک نگرانی فنی به تهدیدی استراتژیک و سیستماتیک ارتقاء داده است و تاب‌آوری سایبری، توانایی است که نه‌تنها برای پیشگیری، بلکه برای مقاومت، بازیابی، و سازگاری در برابر حوادث سایبری به‌ویژه پس از حملات برجسته و اختلالات جهانی مانند جنگ و همه‌گیری کووید-۱۹ به محور اصلی توجه نهادهای مالی در سطح جهانی تبدیل شده است (فدرال رزرو، ۲۰۲۲؛ اف.اس.بی، ۲۰۲۰؛ لینکوف و دیگران، ۲۰۱۸)[11]. ثبات نظام مالی، که جزء جدایی‌ناپذیر اقتصاد کلان است، به تاب‌آوری اجزای کلیدی آن از جمله بانک‌ها و سیستم‌های پرداخت وابسته است. ازاین‌رو نهادهای نظارتی و مالی به‌طور فزاینده‌ای بر تقویت تاب‌آوری سایبری متمرکز شده‌اند تا از اختلالاتی که می‌توانند پیامدهای اقتصادی گسترده داشته باشند، جلوگیری کنند (گزارش ثبات مالی فدرال رزرو ،۲۰۲۴). با وجود پیشرفت‌های امنیتی، رویکردهای سنتی مبتنی‌بر «پیشگیری و حفاظت» در برابر تهدیدات پویا و پیچیده امروز ناکافی بوده است و این ضعف به‌ویژه برای نهادهای مالی سیستماتیک که

1. Shekofteh; López-Pernas
2. Web of Science
3. Scopus
4. Google Scholar
5. VOSviewer
6. UCINET
7. Pajek
8. BibExcel
9. Yao,Ogasawara
10. Bakhmat; Puente.
11. Federal Reserve; FSB; Linkov.

شکست آن‌ها می‌تواند ثبات کل نظام مالی را تهدید کند، نگران‌کننده است (مورر و نلسون، ۲۰۲۱)[1]. نمونهٔ بارز آن حملهٔ سایبری به بانک بنگلادش در سال ۲۰۱۶ بود که محدودیت‌های رویکردهای سنتی را آشکار و ضرورت تاب‌آوری سایبری را برجسته کرد (بلهادی[2] و دیگران، ۲۰۲۱). تاب‌آوری سایبری در ادبیات به‌عنوان ظرفیت مقاومت، بازیابی و سازگاری در برابر شوک‌های خارجی ناشی از ریسک‌های سایبری تعریف شده است. این تعریف، اجتناب‌ناپذیری برخی حملات موفق را به رسمیت می‌شناسد و بر حفظ کارکردهای حیاتی در حین و پس از حوادث تأکید دارد. ریشه‌های این مفهوم در رشته‌های مهندسی، اکولوژی، مدیریت بحران، و نظریهٔ سازمانی است و در زمینهٔ امنیت سایبری مالی نشان‌دهندهٔ گذار از نگاه صرفاً پیشگیرانه به‌سوی ظرفیت سازگاری و بازیابی است (دوپونت[3]، ۲۰۱۹). ادبیات اولیهٔ تاب‌آوری سایبری (۲۰۱۰م–۲۰۱۵م) بیشتر بر جنبه‌های فنی مانند امنیت شبکه، پاسخ به حوادث، و تداوم کسب‌وکار متمرکز بود، اما پس از حوادث برجسته‌ای مانند سرقت بانک بنگلادش، پژوهش‌ها به دیدگاه‌های چندبُعدی گسترش یافت که شامل یادگیری سازمانی، عوامل فرهنگی، و ملاحظات سیستماتیک می‌شد (کوهلر[4] و همکاران، ۲۰۱۹؛ بلهادی و همکاران، ۲۰۲۱). در این راستا، دوپونت (۲۰۱۹) پنج بُعد اصلی تاب‌آوری سایبری در نهادهای مالی را معرفی می‌کند: ۱) تاب‌آوری پویا (سازگاری مداوم)، ۲) تاب‌آوری شبکه‌ای (پاسخ‌های همکاری‌محور)، ۳) تاب‌آوری تمرین‌شده (آزمایش و تمرین منظم)، ۴) تاب‌آوری سازگار (یادگیری مداوم و تکامل اقدامات دفاعی)، و ۵) تاب‌آوری موردمناقشه (برآمده از منافع و دیدگاه‌های رقابتی). این چارچوب، بلوغ تاب‌آوری سایبری را از یک حوزه صرفاً فنی به یک قابلیت سازمانی جامع نشان می‌دهد.

در کنار اهمیت موضوعی، انتخاب پایگاه داده مناسب برای تحلیل علم‌سنجی تاب‌آوری سایبری اهمیت ویژه‌ای دارد. شواهد موجود نشان می‌دهد که اسکوپوس نسبت به وب‌آوساینس و گوگل اسکالر پوشش گسترده‌تر و جامع‌تری از محتوا، رشته‌های علمی، و منابع منطقه‌ای ارائه می‌کند و امکان انجام تحلیل‌های میان‌رشته‌ای دقیق را فراهم می‌سازد. شاخص‌های تأثیرگذاری در اسکوپوس از دقت و قابلیت اعتماد بالایی برخوردارند، کمتر در معرض دست‌کاری هستند و برای تمام منابع در تمامی رشته‌ها قابل دسترسی‌اند. مطالعات تطبیقی نشان داده‌اند که اسکوپوس قادر است روند رشد انتشارات و استنادها را در مقیاس میان‌رشته‌ای به‌طور پایدار پوشش دهد و ابزار مناسبی برای تحلیل‌های کلان و ارزیابی علمی فراهم آورد (باخمت، ۲۰۲۲؛ مارتین-مارتین و دیگران، ۲۰۲۰؛ مارتین-مارتین و دیگران، ۲۰۱۸؛ آدریانس و رنسلی، ۲۰۱۳)[5]. بنابراین، با توجه به جامعیت پوشش، قابلیت دسترسی عملی، دقت شاخص‌ها و ثبات داده‌ها، اسکوپوس منبع دادهٔ اصلی و توصیه‌شده برای تحلیل‌های علم‌سنجی و ارزیابی علمی در سطح ملی و بین‌المللی است و استفاده از آن می‌تواند پایه‌ای معتبر برای پژوهش‌ها و تصمیم‌گیری‌های علمی فراهم آورد.

علاوه‌بر ضرورت علمی، رخدادهای واقعی جدید نیز بر اهمیت بیشتر این موضوع صحه می‌گذارند. برای نمونه، در جریان جنگ ۱۲ روزه بین ایران و اسرائیل (ژوئن ۲۰۲۵)، فضای سایبری ایران به یکی از جبهه‌های مهم درگیری تبدیل شد، به‌گونه‌ای که گروه هکری گنجشک درنده[6] حملات مستقیم علیه زیرساخت‌های بانکی و مالی کشور انجام دادند. بانک‌های سپه و پاسارگاد متحمل اختلالات گسترده در سرویس‌های بانکداری آنلاین، کارت اعتباری، و دستگاه‌های خودپرداز شدند و خدمات بانکی برای میلیون‌ها مشتری برای چند روز مختل شد. شدت حملات به گونه‌ای بود که حتی با استفاده از سایت‌های پشتیبان(بازیابی از فاجعه)[7]، برخی

1. Maurer & Nelson
2. Belhadi
3. Benoît Dupont
4. Köhler
5. Martín-Martín, Adriaanse & Rensleigh
6. Predatory Sparrow
7. Disaster Recovery Sites

بانک‌ها قادر به بازیابی کامل داده‌ها نبودند (اقتصاد آنلاین، ۱۴۰۴). همچنین، حمله به صرافی رمزارز نوبیتکس[1] و سرقت حدود ۹۰ میلیون دلار رمزارز، همراه با سوزاندن[2] دارایی‌ها، نشان داد که هدف مهاجمان نه‌تنهاایجاد اختلال مقطعی، بلکه تضعیف اعتماد عمومی به نظام بانکی و آزمودن تاب‌آوری سایبری کشور بوده است. این وقایع به وضوح ضعف‌های موجود در بازیابی داده‌ها، وابستگی به زیرساخت‌های مرکزی آسیب‌پذیر، و کمبود سایت‌های بازیابی غیرمتمرکز قابل اعتماد را نشان داد و ضرورت ارتقاء تاب‌آوری سایبری نظام مالی، به‌ویژه در شرایط جنگ و بحران، را برای سیاست‌گذاران، ناظران امنیتی، و مدیران بانکی به یک اولویت محوری تبدیل کرد (حملهٔ سایبری به نوبیتکس ،۱۴۰۴).

بر این اساس، این پژوهش با بهره‌گیری از تحلیل علم‌سنجی، به بررسی نظام‌مند روندهای پژوهشی، مشارکت‌کنندگان کلیدی، تکامل موضوعی، و شبکه‌های همکاری در زمینهٔ تاب‌آوری سایبری برای سیستم‌های مالی و بانکی در بازهٔ زمانی ۲۰۱۸ تا ۲۰۲۵ می‌پردازد. هدف این پژوهش، ترسیم نقشهٔ جامعی از این حوزه دانش و ارائهٔ بینش‌هایی برای تقویت سیاست‌گذاری، تخصیص منابع، و تدوین راهبردهای عملی در صنعت مالی است. برای دستیابی به این هدف، پژوهش حاضر به دنبال پاسخ به سؤالات کلیدی زیر است:

۱. روند انتشار مقالات علمی در حوزهٔ تاب‌آوری سایبری در نظام های مالی و بانکی طی دهه اخیر چگونه بوده و چه موضوعاتی بیشترین فراوانی را در ادبیات این حوزه داشته‌اند؟
۲. کدام مؤسسات، کشورها، و پژوهشگران در تولید دانش علمی مرتبط با تاب‌آوری سایبری در نظام‌های مالی و بانکی بیشترین نقش و تأثیرگذاری را داشته‌اند؟
۳. الگوهای همکاری علمی میان پژوهشگران، مؤسسات، و کشورها در سطح بین‌المللی چگونه شکل گرفته‌اند؟ (با تمرکز بر شبکه‌های هم‌نویسندگی و هم‌استنادی).
۴. چه خوشه‌های موضوعی کلیدی و روندهای نوظهوری در ادبیات علمی تاب‌آوری سایبری قابل شناسایی هستند؟
۵. مهمترین شکاف‌های پژوهشی در حوزهٔ تاب‌آوری سایبری نظام‌های مالی و بانکی چیست و نتایج علم‌سنجی چگونه می‌تواند جهت‌گیری پژوهش‌های آینده و سیاست‌گذاری‌ها را هدایت کند؟

۲. پیشینه نظری

در دههٔ اخیر تاب‌آوری سایبری به‌تدریج از یک مفهوم مکمل به چارچوبی محوری برای مدیریت ریسک و پایداری در محیط‌های دیجیتال ارتقاء یافته است. دوپونت (۲۰۱۹) نخستین گام را با تأکید بر ناکارآمدی صرفِ پیشگیری و حفاظت و پیشنهاد سه راهبرد نهادی ـ پیشگامی صنعت امنیت، گنجاندن مفاهیم تاب‌آوری در استانداردها و الزامات نظارتی ـ برداشت. کوجوکارو[3] (۲۰۲۵) با معرفی یک چارچوب مفهومی جامع، ابعاد راهبرد نظارتی، حکمرانی، مشارکت ریسک، و بازخورد سازگار را به‌عنوان ارکان اساسی تاب‌آوری در بخش مالی شناسایی کرد. گوندوزایلی[4] (۲۰۲۵) پیوند میان تاب‌آوری سایبری و پایداری عملیات بازاریابی دیجیتال را با تمرکز بر محافظت از داده‌ها، تداوم عملیات، و اعتماد مشتری آشکار ساخت. الحربی[5] (۲۰۲۵) با تحلیل تجربهٔ عربستان سعودی در سال‌های ۲۰۱۲ تا ۲۰۲۴ نشان داد که سیاست‌های انعطاف‌پذیر، نهادهای تخصصی، و همکاری‌های بین‌المللی چگونه جایگاه یک کشور را در

1. Nobitex
2. Burn
3. Cojocaru
4. Gündüzyeli
5. Alharbi

شاخص‌های امنیت سایبری ارتقاء می‌دهند. سید و دیگران (۲۰۲۵) با چارچوب کارایی، تست نفوذ مبتنی‌بر تهدید را برای مؤسسات مالی افزایش دادند و صفیترا و دیگران (۲۰۲۴) تاب‌آوری سایبری را به‌عنوان چارچوبی پویا شامل سازوکارهای رمزنگاری داده‌ها، پایش شبکه، و سنجش آمادگی سازمانی تبیین کردند. در ادامه، ساها و واوتشا ساها (۲۰۲۴) با توسعهٔ ماشین‌حساب تاب‌آوری سایبری افق تازه‌ای برای تخصیص بهینهٔ بودجهٔ امنیتی در کسب‌وکارهای کوچک و متوسط گشودند و گادبول و دیگران (۲۰۲۲) بر نقش رفتار کارکنان در بازیابی سریع از حملات سایبری و پُر کردن شکاف مطالعات فنی‌محور گذشته تأکید کردند. این شواهد جمعی نه‌تنها پویایی و بلوغ روزافزون این حوزه را نشان می‌دهد، بلکه مسیر حرکت آن به‌سوی تلفیق ابعاد فنی، انسانی، و سازمانی و تبدیل‌شدن به یک پارادایم کلیدی برای پایداری و مزیت رقابتی در عصر دیجیتال را نیز ترسیم می‌کند. جدول۱ خلاصه از پیشینهٔ نظری مقالات کارشده در این حوزه است.

جدول ۱. پیشینهٔ پژوهش

نویسنده / سال	موضوع	نتایج
بنوا دوپونت (۲۰۱۹)	تاب‌آوری سایبری مؤسسات مالی: اهمیت و قابلیت اجرا	یافته‌های مقالهٔ بنوا دوپونت نشان می‌دهد که با توجه به غیرقابل اجتناب بودن حملات سایبری پیشرفته، رویکرد تاب‌آوری سایبری یک جایگزین مکمل و ضروری برای رویکرد ناکافی «پیشگیری و حفاظت» است. پژوهش او سه راهکار نهادی را برای توسعهٔ این تاب‌آوری برمی‌شمارد: پیشگامی صنعت امنیت، گنجاندن مفاهیم آن در استانداردها، و ایجاد الزامات نظارتی، که باید در مجموعه ابزار مدیران ریسک ادغام شوند.
آندرا کوجوکارو (۲۰۲۵)	هم‌ترازسازی مقررات و حکمرانی برای تاب‌آوری سایبری: یک چارچوب نظری برای بخش مالی بریتانیا	یک چارچوب مفهومی یکپارچه ارائه می‌دهد که چهار بُعد راهبرد نظارتی، اجرای حکمرانی، مشارکت ریسک، و بازخورد سازگار را به‌عنوان ارکان اصلی تاب‌آوری سایبری در بخش مالی مرتبط می‌سازد. یافته‌ها نشان می‌دهد که تاب‌آوری سایبری یک فرایند مستمر است که از تعامل بین طراحی نهادی و نظارت شکل می‌گیرد و هم‌سویی سازوکارهای داخلی مؤسسات با الزامات نظارتی در حال تحوّل را ضروری می‌داند. این چارچوب هم برای درک پویایی‌های حکمرانی و نظارت و هم برای راهنمایی عملی مؤسسات در تقویت تاب‌آوری کاربرد دارد.
بورا گوندوزالپلی (۲۰۲۵)	تاب‌آوری سایبری در بازاریابی دیجیتال در چارچوب مدیریت پایدار	نتایج پژوهش بورا گودوزالپلی نشان می‌دهد تاب‌آوری سایبری در تضمین پایداری عملیات بازاریابی دیجیتال نقش حیاتی ایفا می‌کند، به‌طوری‌که ادغام راهبردهای سایبری در سه حوزهٔ محافظت از داده‌ها، تداوم عملیات، و جلب اعتماد مشتری، امکان مقابله مؤثر با تهدیدات سایبری را فراهم می‌سازد. این رویکرد نه‌تنها امنیت عملیاتی را افزایش می‌دهد، بلکه به‌عنوان یک عامل کلیدی در دستیابی به پایداری بلندمدت و حفظ مزیت رقابتی در فضای دیجیتال عمل می‌کند. در نهایت، چارچوب ارائه‌شده در این مطالعه می‌تواند به‌عنوان راهنمای عملی برای بازاریابان و سیاست‌گذاران در راستای هم‌سوسازی اهداف امنیت سایبری با الزامات پایداری استفاده شود.
فاطمه الحربی (۲۰۲۵)	دوازده سال تاب‌آوری سایبری: تحلیل حملات سایبری در عربستان سعودی۲۰۱۲-۲۰۲۴	در طول دوازده سال گذشته، عربستان سعودی با افزایش چشمگیر حملات سایبری روبه‌رو بوده که خسارات مالی قابل توجه و تهدیدات جدی برای امنیت ملی این کشور به همراه داشته است. پاسخ‌های راهبردی دولت از جمله تأسیس نهادهای تخصصی امنیت سایبری، تصویب قوانین پیشرفته، و ایجاد مشارکت‌های بین‌المللی، منجر به ارتقاء چشمگیر جایگاه این کشور در شاخص‌های جهانی امنیت سایبری شده است. با این حال، تهدیدات پیچیده و دائماً در حال تغییر، لزوم تدوین سیاست‌های انعطاف‌پذیر، تقویت همکاری‌های بین‌المللی، و حفظ آمادگی مستمر برای حفاظت از زیرساخت‌های دیجیتال را بیش از پیش ضروری ساخته است.
الیاس سید[2] و دیگران (۲۰۲۵)	تاب‌آوری سایبری با استفاده از چارچوب : ASFA تست نفوذ مبتنی بر تهدید منطبق با مقرراتDORA[1]	با توجه به افزایش رخدادهای سایبری در بخش مالی، مطالعهٔ الیاس سید و همکاران بر اهمیت درنظرگیری هم‌زمان ابعاد فنی، انسانی، و سازمانی در سیستم‌های اجتماعی-فنی تأکید می‌کند. یافته‌ها نشان می‌دهد که استفاده از چارچوب یکپارچهٔ پایش امنیت شامل ابعاد اجتماعی، سایبری، و فیزیکی توانایی مؤسسات مالی در انجام آزمون نفوذ مبتنی‌بر تهدید و مقابله با بحران‌های سایبری را به‌طور چشمگیری افزایش می‌دهد. همکاری با یک مؤسسهٔ مالی پیشرو، کارایی عملیاتی این چارچوب در شناسایی و کاهش آسیب‌پذیری‌های پیچیده را تأیید کرده است.

1. Digital Operational Resilience Act
2. Seid

نویسنده / سال	موضوع	نتایج
صفیترا[1] و دیگران (۲۰۲۴)	وضعیت تاب‌آوری سایبری: پیشرفت‌ها و جهت‌های آینده	تاب‌آوری سایبری به‌عنوان یک چارچوب پویا شامل شناسایی تهدید، محافظت، تشخیص، پاسخ و بازیابی، سازمان‌ها را در مدیریت مؤثر ریسک‌های سایبری توانمند می‌سازد. بهبود این تاب‌آوری مستلزم به‌کارگیری سازوکارهایی مانند رمزنگاری داده‌ها، پایش شبکه، و توسعهٔ شاخص‌های سنجش آمادگی سازمانی است. آیندهٔ این حوزه وابسته به ادغام فناوری‌های پیشرفته، تقویت همکاری، و سرمایه‌گذاری در آموزش است تا یک محیط دیجیتال امن و مقاوم ایجاد شود.
بینیتا ساها واوتشا ساها[2] (۲۰۲۴)	ماشین حساب تاب‌آوری سایبری: تحوّلی برای کسب‌وکارهای کوچک و متوسط در تخصیص مؤثر بودجه امنیت فناوری اطلاعات	یک ماشین حساب تاب‌آوری سایبری را برای کمک به کسب‌وکارهای کوچک و متوسط در تخصیص بهینهٔ بودجهٔ امنیتی با در نظرگیری عواملی مانند نوع کسب‌وکار و سطح تحمل ریسک طراحی کرده است. یافته‌ها نشان می‌دهد این ابزار به تصمیم‌گیری آگاهانه در زمینهٔ سرمایه‌گذاری امنیتی کمک کرده و وضعیت دفاع سایبری این کسب‌وکارها را به‌طور قابل توجهی بهبود می‌بخشد. توسعهٔ چنین ابزارهایی برای ایجاد دفاع‌های امنیتی پایدار ضروری بوده و نیازمند پژوهش‌های بیشتر برای افزایش دقت و کارایی آن است.
تانوی گادبول[3] و دیگران (۲۰۲۲)	تدوین چارچوبی برای سنجش رفتار تاب‌آوری سایبری کارکنان بانک‌های هند	با توجه به افزایش جرائم سایبری در بانک‌های هند، بر ضرورت تاب‌آوری سایبری کارکنان به‌عنوان عامل کلیدی در مقابله با تهدیدات تأکید می‌کند. چارچوب پیشنهادی با تمرکز بر سنجش رفتار تاب‌آوری سایبری کارکنان، شکاف موجود در مطالعات پیشین که بیشتر بر جنبه‌های فنی متمرکز بوده‌اند را پُر می‌کند. یافته‌ها نشان می‌دهند که بهبود رفتار کارکنان در رویارویی با حملات سایبری، نقش تعیین‌کننده‌ای در سرعت بازیابی بانک‌ها از آسیب‌پذیری‌ها دارد.

۳. روش‌شناسی

۱. رویکرد پژوهش: این مطالعه با بهره‌گیری از تحلیل علم‌سنجی به بررسی روندهای پژوهشی در زمینهٔ تاب‌آوری سایبری در بخش مالی و بانکی می‌پردازد. تحلیل علم‌سنجی به دلیل توانایی در شناسایی الگوهای انتشاراتی، روابط میان نویسندگان، و حوزه‌های موضوعی، ابزاری مناسب برای ترسیم چشم‌انداز علمی یک حوزهٔ‌نوظهور است (دانتو و همکاران[4]، ۲۰۲۱).

۲. منبع داده: پایگاه داده اسکوپوس به‌عنوان یکی از جامع‌ترین و معتبرترین پایگاه‌های نمایه سازی نشریات علمی انتخاب شد. این پایگاه پوشش گسترده‌ای در حوزهٔ مدیریت، بانکداری، امنیت سایبری، و سیستم‌های اطلاعاتی دارد و استاندارد طلایی در انجام مرورهای نظام‌مند و تحلیل‌های کتاب‌سنجی محسوب می‌شود (برنهام[5]، ۲۰۰۶).

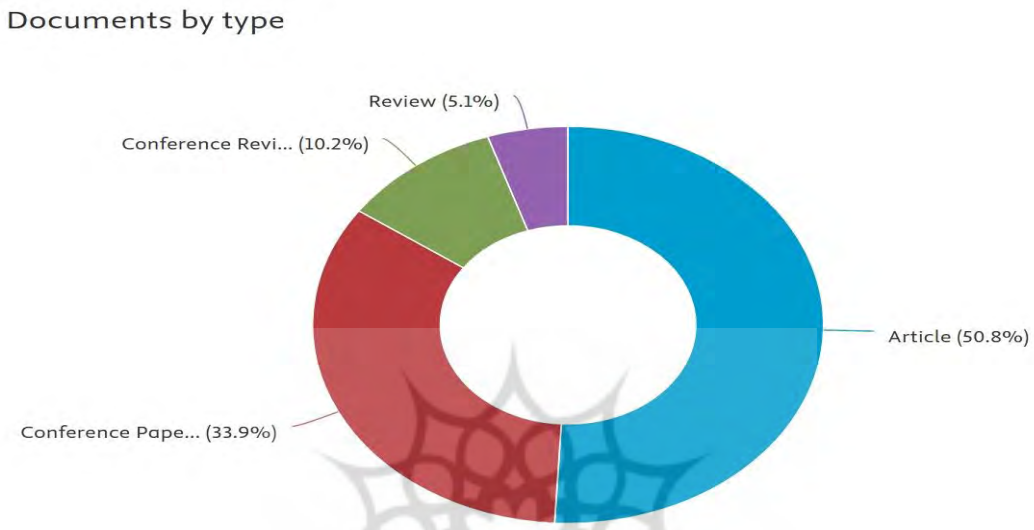
۳. استراتژی جست‌وجو: جست‌وجوی اولیه با تمرکز بر واژه‌های کلیدی اصلی انجام شد. عبارت‌های کلیدی شامل ترکیبات مختلف واژهٔ «Cyber Resilience» ، اصطلاحات مرتبط با «Banking» و «Financial» بود. جست‌وجو به صورت زیر در اسکوپوس اجرا شد:

(TITLE-ABS-KEY("Cyber Resilience") OR TITLE-ABS-KEY("CyberResilience") OR TITLE-ABS-KEY("Cyber_Resilience") AND TITLE-ABS-KEY("Banking") OR TITLE-ABS-KEY("Financial")) AND (LIMIT-TO (LANGUAGE,"English")) AND (LIMIT-TO (DOCTYPE,"ar") OR LIMIT-TO (DOCTYPE,"cp") OR LIMIT-TO (DOCTYPE,"cr") OR LIMIT-TO (DOCTYPE,"re")) AND PUBYEAR > 2018 AND PUBYEAR < 2025

این عبارت جست‌وجو با هدف پوشش تمام اشکال نگارشی «تاب‌آوری سایبری» و حوزهٔ «بانکداری و مالی» طراحی شد تا جامعیت داده‌ها حفظ شود.

1. Safitra
2. Saha, B., & Saha, U.
3. Godbole
4. Donthu
5. Burnham

۴. معیارهای ورود و خروج: در این پژوهش، معیارهای ورود شامل مقالات علمی، مقالات مروری، مقالات مروری کنفرانسی، و مقالات کنفرانسی در گروه بود. درصد هر نوع سند در شکل۱ به زبان انگلیسی، در بازهٔ زمانی ۲۰۱۸ تا ۲۰۲۵ و با تمرکز مشخص بر موضوع تاب‌آوری سایبری در نظام‌های مالی و بانکی نشان داده شده است. در مقابل، معیارهای خروج شامل مقالات غیرانگلیسی، گزارش‌های غیرعلمی، داده‌های تکراری، و پژوهش‌هایی بود که تنها به امنیت سایبری عمومی پرداخته و پیوندی با حوزهٔ مالی یا بانکی نداشتند.



شکل ۱. نوع اسناد تحلیل شده

۵. فرایند غربالگری و آماده سازی داده‌ها: ابتدا نتایج جست‌وجو از پایگاه علمی اسکوپوس استخراج شد. داده‌های خام استخراج‌شده با استفاده از نرم‌افزار OpenRefine پاک‌سازی و یکپارچه‌سازی شدند تا خطاهای ناشی از ناهمگونی اسامی نویسندگان، مؤسسات، و کلیدواژه‌ها حذف شود. سپس داده‌ها برای تحلیل شبکه‌ای و مصوّر سازی آماده شدند. برای تحلیل روابط هم‌نویسندگی و هم‌واژگانی از نرم‌افزار VOSviewer بهره گرفته شد که امکان شناسایی ساختارهای مفهومی، خوشه‌های موضوعی، و روابط میان کشورها و مؤسسات را فراهم می‌سازد. افزون‌بر این، برای تحلیل‌های تکمیلی، نمودارهای توصیفی و محاسبات آماری از زبان برنامه‌نویسی Python و کتابخانه‌های تخصصی آن شامل Pandas، NumPy و Matplotlib استفاده شد. ترکیب این ابزارها تصویری جامع از وضعیت علم‌سنجی این حوزه را در سطوح زمانی، جغرافیایی، و مفهومی ارائه کرده است. این گام تضمین می‌کند که نتایج نهایی بازتاب دقیقی از وضعیت پژوهش در این حوزه باشد. خلاصهٔ از روش‌شناسی این پژوهش در جدول ۲ آمده است.

جدول ۲. خلاصهٔ روش پژوهش

مؤلفه	توضیحات
پایگاه داده	Scopus
کلیدواژه‌ها	“Cyber Resilience”, “CyberResilience”, “Cyber_Resilience” AND “Banking” OR “Financial”
بازه زمانی	۲۰۱۸-۲۰۲۵
نوع مدارک	مقاله پژوهشی(ar) ، مقاله مروری(re) ، مقاله کنفرانسی(cp) ، مقاله مروری کنفرانسی(cr)
زبان	انگلیسی

معیار ورود	ارتباط مستقیم با تاب‌آوری سایبری در بانکداری/ مالی
معیار خروج	مقالات غیرانگلیسی، داده‌های تکراری یا نامرتبط
ابزار تحلیل	python ،VOSviewer
روش پاک‌سازی	حذف تکراری‌ها، استانداردسازی نام‌ها، و کلیدواژه‌ها

۴. یافته‌های پژوهش

تحلیل روند رشد مقالات در پاسخ به قسمت اول سؤال ۱ و با توجه به شکل ۲ به شرح ذیل است:

- **دورهٔ ۲۰۱۸–۲۰۲۰:** پژوهش‌ها هنوز در مرحلهٔ شکل‌گیری و تمرکز اصلی بر مفاهیمی مثل امنیت سایبری، فرهنگ سایبری در بانک‌ها، و پایه‌گذاری مدل‌های تاب‌آوری بود
- **دورهٔ ۲۰۲۱–۲۰۲۳:** یک رکود کوتاه در ۲۰۲۱ ولی بعد بازگشت به رشد، در این مقطع، مطالعات موردی و مدیریت سیستم‌های تاب‌آور گسترش یافت.
- **دورهٔ ۲۰۲۴–۲۰۲۵:** جهش انفجاری در ۲۰۲۴ نشان می‌دهد که تاب‌آوری سایبری در نظام‌های مالی به یک حوزهٔ پژوهشی اصلی تبدیل شده است. دلایل آن می توانند افزایش حملات سایبری به بانک‌ها، گسترش فناوری‌های جدید (پرداخت‌های دیجیتال، بانکداری باز)، و فشارهای قانونی و مقرراتی (مانند الزامات GDPR و Basel III در امنیت داده) باشد.

روند کلی یک مسیر صعودی با جهش ناگهانی در سال‌های اخیر را نشان می‌دهد. پیش‌بینی آینده بیانگرِ آن است که این روند صعودی ادامه خواهد داشت. این موضوع برای پژوهش اهمیت بالایی دارد، زیرا نشان می‌دهد که حوزهٔ تاب‌آوری سایبری در نظام‌های مالی و بانکی به‌تازگی به یک حوزهٔ داغ[1] تبدیل شده و هنوز ظرفیت بالایی برای کار پژوهشی دارد.

شکل ۲. روند زمانی انتشار مقالات این حوزه

تحلیل موضوعی مقالات در پاسخ به قسمت دوم سؤال ۱ و با توجه به جدول ۳ تمرکز مقالات منتشرشده طی سال‌های ۲۰۱۸ تا ۲۰۲۵ در حوزهٔ تاب‌آوری سایبری در نظام‌های مالی و بانکی نشان می‌دهد که ادبیات این حوزه مسیر تکاملی مشخصی را پیموده

1. Hot Topic

است. در ابتدای دوره (۲۰۱۸ و ۲۰۱۹)، پژوهش‌ها بیشتر بر موضوعات نوظهور مانند تاب‌آوری فردی در برابر حملات سایبری، امنیت انرژی‌های تجدیدپذیر، و شکل‌دهی به فرهنگ امنیت سایبری در بانک‌ها تمرکز داشتند. این مقالات با استنادات نسبتاً بالا (۴۳ بار برای مطالعه هوآ[1] و همکاران (۲۰۱۸) و ۲۵ بار برای ورنوت[2] و همکاران (۲۰۱۸) و۱۶ بار برای ماروتا[3] و همکاران (۲۰۱۹)) پایه‌های اولیه توجه علمی را به ابعاد فردی و سازمانی تاب‌آوری سایبری بنا نهادند. هم‌زمان، پژوهش دوپونت[4] (۲۰۱۹) با ۷۳ استناد به تبیین اهمیت تاب‌آوری سایبری در مؤسسات مالی پرداخت و به‌نوعی «دستور کار پژوهشی» در این حوزه را تثبیت کرد.

با ورود به سال‌های ۲۰۲۰ تا ۲۰۲۱، ادبیات به‌وضوح به سمت تدوین چارچوب‌ها و شاخص‌های سنجش تاب‌آوری حرکت کرد. مقاله ویشوناس[5] و همکاران (۲۰۲۰) با ۷۹ استناد درباره «بهداشت سایبری» و مقاله انارلی[6] و همکاران (۲۰۲۰)با ۶۳ استناد درباره «مدیریت سیستم‌های تاب‌آور» نشان می‌دهند که تمرکز اصلی از بحث‌های مفهومی صرف به سمت ابزارهای اندازه‌گیری و مدیریت سیستماتیک تغییر کرده است. در همین دوره، گروندال[7] و همکاران (۲۰۲۱) با مطالعهٔ موردی در بحران کووید-۱۹ (۳۰ استناد) این حوزه را از نظریه به عمل پیوند زد و اهمیت تاب‌آوری سایبری در شرایط بحرانی را مستند ساخت.

از سال ۲۰۲۴ به بعد، پژوهش‌ها به‌سمت گسترش کاربردی‌تر و پیوند تاب‌آوری سایبری با مدیریت زنجیره تأمین و بازارهای مالی پساکرونا حرکت کرده‌اند. نمونهٔ بارز این تغییر، مقاله هربرگر[8] و همکاران (۲۰۲۴) دربارهٔ قابلیت‌های پویا در زنجیره تأمین (۱۵ استناد) و مقالهٔ Prabhu et al. (۲۰۲۴) دربارهٔ بازارهای مالی هند در دورهٔ پساکرونا (۱۲ استناد) است. این تغییرات نشان می‌دهد که پژوهشگران اکنون به‌دنبال یکپارچه‌سازی ابعاد فناورانه، سازمانی، و زنجیره تأمین هستند.

این مسیر تکاملی نشان می‌دهد که ادبیات حوزهٔ تاب‌آوری سایبری از یک مرحلهٔ مفهومی و پراکنده در ابتدای دوره به‌سمت چارچوب‌های اندازه‌گیری، مدیریت سیستم‌ها، مطالعات بحران، و سرانجام تلفیق با فناوری‌های نوین و زنجیره تأمین حرکت کرده است. چنین تحوّلی بیانگر بلوغ تدریجی دانش و حرکت آن به‌سمت رویکردهای میان‌رشته‌ای و کاربردی‌تر است.

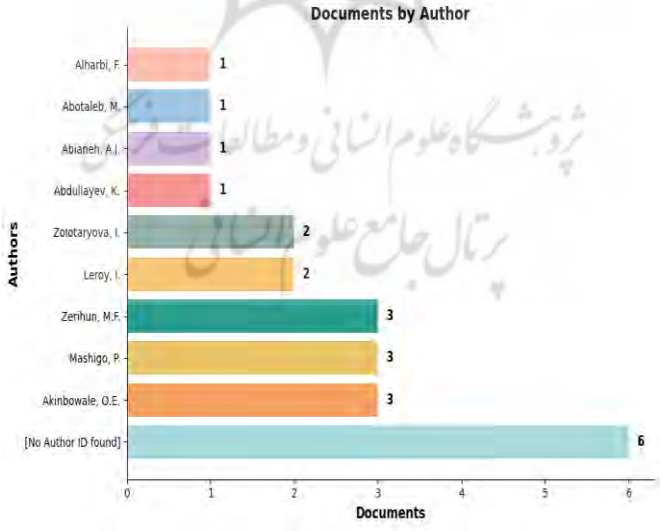
جدول ۳. ده مقالهٔ برتر

Authors/ Year	Title	Cited by	DOI
Vishwanath et al. (2020)	Cyber hygiene: The concept, its measure, and its initial tests	79	https://doi.org/10.1016/j.dss.2019.113160
B., Dupont, Benoît(2019)	The cyber-resilience of financial institutions: Significance and applicability	73	https://doi.org/10.1093/cybsec/tyz013
Annarelli et al. (2020)	Understanding the management of cyber resilient systems	63	https://doi.org/10.1016/j.cie.2020.106829
Hua et al. (2018)	Are we ready for cyberterrorist attacks?—Examining the role of individual resilience	43	https://doi.org/10.1016/j.im.2018.04.008

1. Hua
2. Vernotte
3. Marotta
4. Dupont
5. Vishwanath
6. Annarelli
7. Groenendaal
8. Herburger

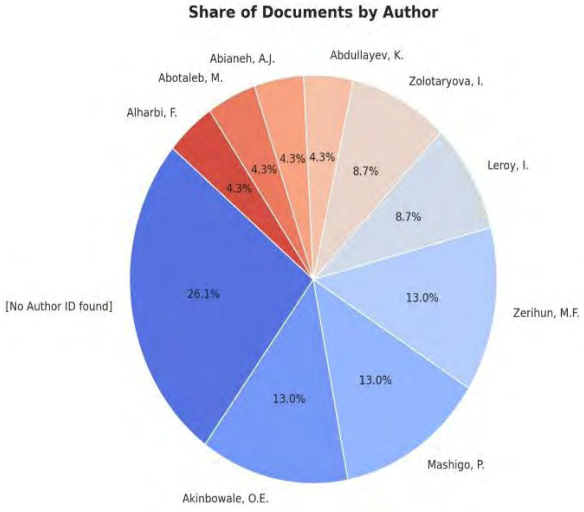
Groenendaal et al. (2021)	Cyber resilience during the COVID-19 pandemic crisis: A case study	30	https://doi.org/10.1111/1468-5973.12360
Vernotte et al. (2018)	Load balancing of renewable energy: a cyber security analysis	25	https://doi.org/10.1186/s42162-018-0010-x
Marotta et al. (2019)	A culture of cybersecurity at Banca popolare di sondrio	16	https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/24
Herburger et al. (2024)	Building supply chain resilience to cyber risks: a dynamic capabilities perspective	15	https://doi.org/10.1108/SCM-01-2023-0016
Hagan et al. (2019)	Enhancing Security and Privacy of Next-Generation Edge Computing Technologies	14	https://doi.org/10.1109/PST47121.2019.8949052
Prabhu et al.(2024)	Cyber Resilience: Safeguarding India's Markets in the Post-Pandemic Cyber Landscape	12	https://doi.org/10.1109/ICIPTM59628.2024.10563229

تحلیل نمودارهای ذیل در پاسخ به سؤال دوم پژوهش به شرح زیر است: با توجه به نمودار ۳ در سطح فردی نیز مشاهده می‌شود که بیشترین تعداد اسناد به نام مشخصی منتسب نشده و در دستهٔ [No Author ID found] قرار گرفته است (۶ سند). با این حال، سه پژوهشگر با نام‌های اکین‌بوآل، ماشیگو و زریهان[1] هرکدام با سه سند در زمرهٔ فعال‌ترین نویسندگان قرار دارند. پس از آن، پژوهشگرانی چون زولوتاریوا و لروی[2] با دو سند و دیگر نویسندگان با تنها یک سند فعالیت محدودتری داشته‌اند. این نتایج بیانگر آن است که تولید دانش در این حوزه علاوه‌بر تمرکز بر چند پژوهشگر کلیدی، به شکل پراکنده میان سایر نویسندگان نیز توزیع شده است. شکل ۴ سهم هر نویسنده را به درصد نشان می‌دهد.



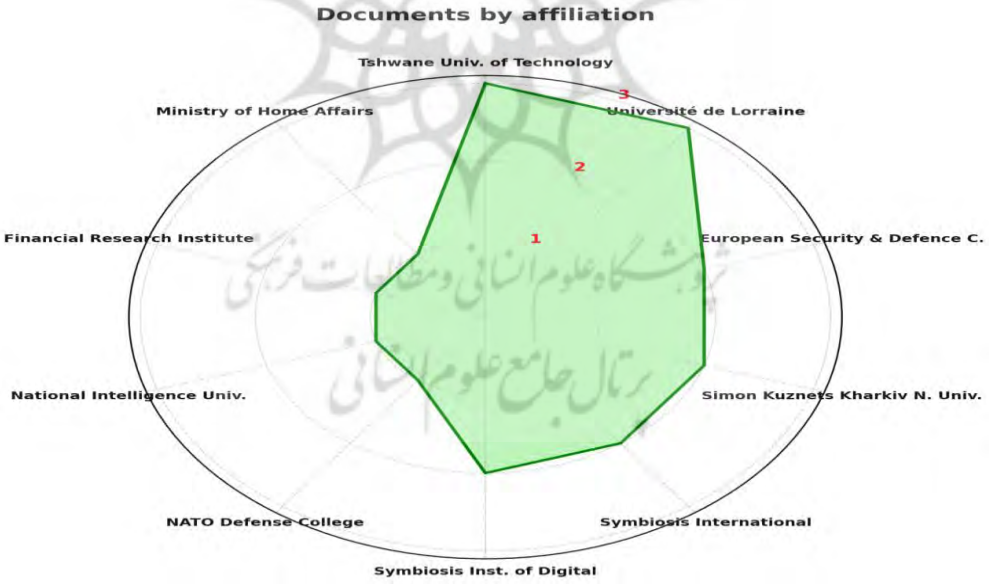
شکل ۳. ده نویسنده برتر

1. Akinbowale, Mashigo, Zerihun
2. Zolotaryova, Leroy



شکل ۴. درصد سهم هر نویسنده

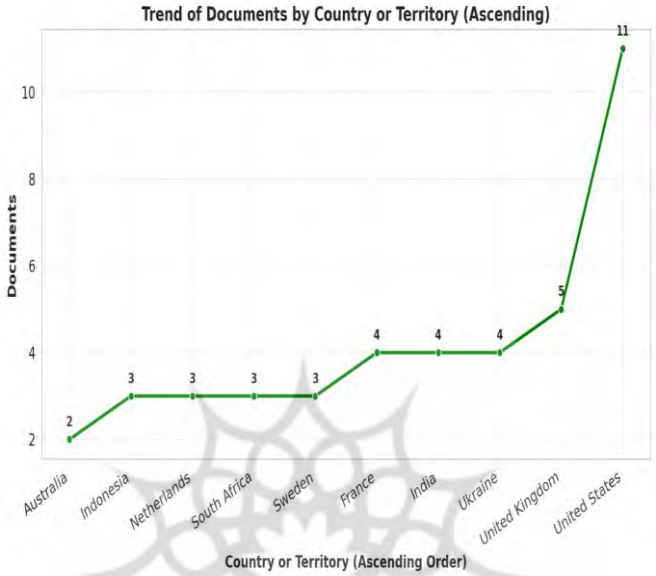
با توجه به شکل ۵، از منظر نهادی، دو مؤسسه دانشگاه فناوری تیشوان[1] و دانشگاه دولورین[2] با انتشار سه سند بیشترین نقش را در تولید دانش ایفا کرده‌اند. در ادامه، مؤسساتی نظیر کالج امنیت و دفاع اروپا[3]، سایمون خازنت کارکیو[4] هرکدام با دو سند در سطح میانی قرار دارند. سایر مؤسسات تنها یک سند منتشر کرده‌اند. این یافته‌ها نشان می‌دهد که اگرچه تولید دانش میان مؤسسات مختلف پراکنده است، اما برخی دانشگاه‌ها و مراکز تحقیقاتی نقش پررنگ‌تری ایفا کرده‌اند.



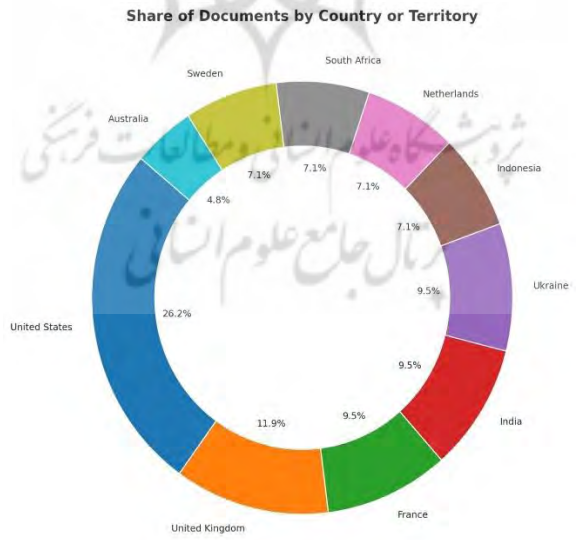
شکل ۵. ده مؤسسه (دانشگاه) برتر

1. Tshwane University of Technology
2. Université de Lorraine
3. European Security & Defense College
4. Simon Kuznets Kharkov N. Univ

در سطح کشورها شکل ۶ نشان می‌دهد که ایالات متحده با ۱۱ سند بیشترین سهم را در تولید دانش علمی مرتبط با تاب‌آوری سایبری در نظام‌های مالی و بانکی دارد و در جایگاه نخست قرار گرفته است. پس از آن، بریتانیا با پنج سند و کشورهایی چون فرانسه، هند، و اوکراین هرکدام با چهار سند در رتبه‌های بعدی قرار دارند. سایر کشورها از جمله استرالیا، اندونزی، هلند، آفریقای جنوبی، و سوئد مشارکت محدودتری داشته‌اند. این روند نشان می‌دهد که تمرکز اصلی دانش تولیدشده در این حوزه بر ایالات متحده و اروپا است، هرچند حضور برخی کشورها از آسیا و آفریقا نیز قابل مشاهده است. شکل ۷ سهم هر کشور را به درصد نشان می دهد.



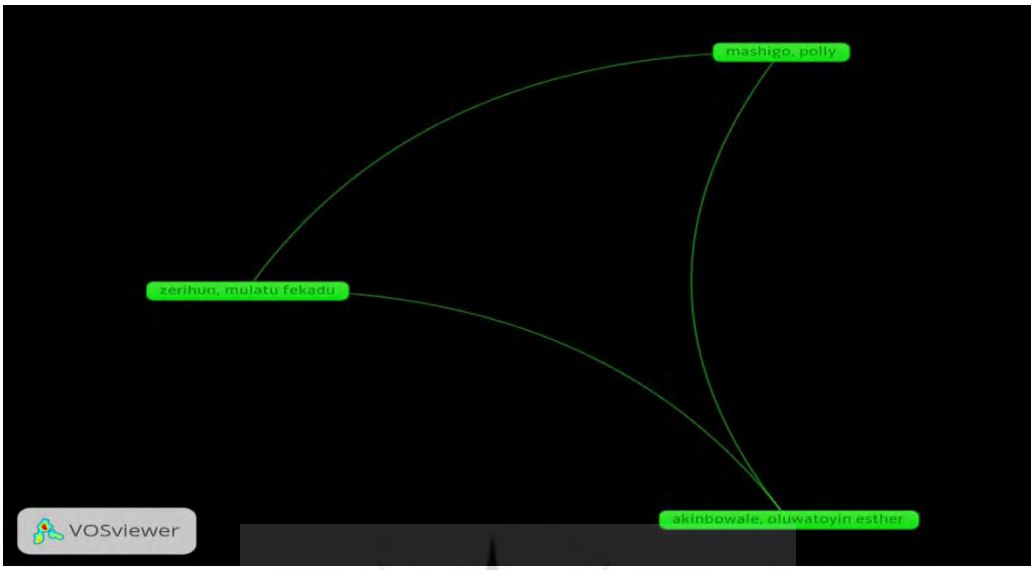
شکل ۶. ده کشور برتر در این حوزه



شکل۷. درصد سهم هر کشور از پژوهش

تحلیل شکل‌های ذیل در پاسخ به سؤال سوم پژوهش به شرح زیر استدر شکل ۸ شبکهٔ همکاری میان سه پژوهشگر زریهان، آکین‌بوال و ماشیگو مشاهده می‌شود که روابط آن‌ها کاملاً نزدیک و دوطرفه است. این ساختار کوچک اما منسجم نشان‌دهندهٔ

همکاری مستقیم و پایدار میان نویسندگان است که برخلاف گستردگی روابط در سطح ملی، از تراکم بیشتری برخوردار بوده و کیفیت همکاری‌ها را در مقیاس خرد تقویت می‌کند.



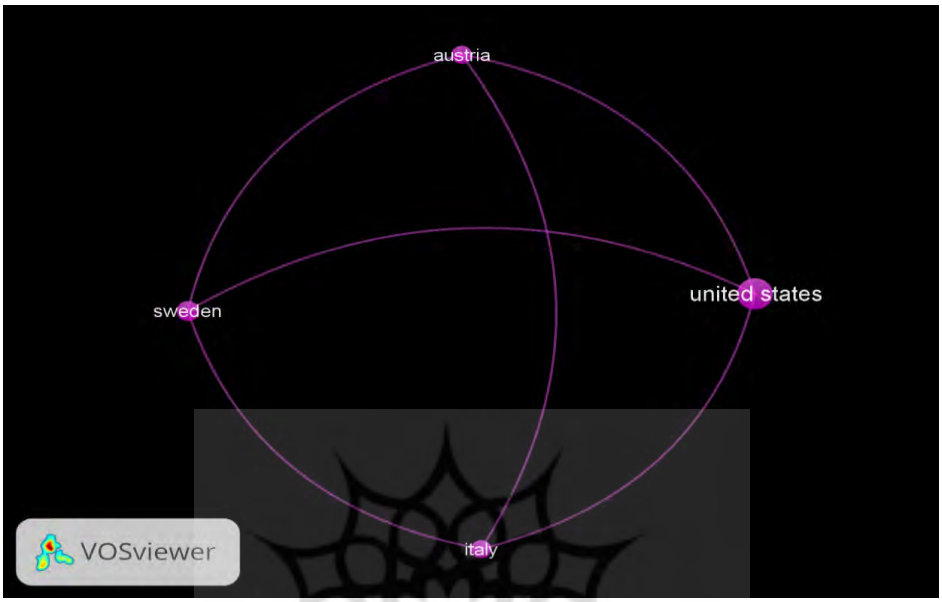
شکل ۸. شبکهٔ همکاری نویسندگان

همکاری مؤسسات: در سطح مؤسسات، شکل ۹ شبکهٔ همکاری محدودتر و متشکل از سه نهاد کالج امنیت و دفاع اروپا، دانشگاه دولورین نانسی[1] و سایمون خازنت کارکیو است. این سه مؤسسه در قالب یک خوشهٔ کوچک با یکدیگر همکاری کرده‌اند و روابط علمی آن‌ها به صورت متوازن اما محدود شکل گرفته است. این الگو نشان می‌دهد که برخلاف سطح کشورها، تمرکز همکاری‌ها در سطح سازمانی بر تعداد اندکی نهاد علمی استوار است.

شکل ۹. شبکهٔ همکاری دانشگاه ها

1. Université de Lorraine Nancy

همکاری کشورها: شبکهٔ همکاری میان کشورها در شکل ۱۰ نشان می‌دهد که ایالات متحده نقش محوری و پررنگ‌تری در تعاملات علمی دارد و بیشترین ارتباط را با کشورهای اروپایی از جمله ایتالیا، سوئد، و اتریش برقرار کرده است. این الگو بیانگر آن است که همکاری‌های علمی در سطح بین‌المللی بیشتر در محور آمریکا-اروپا شکل گرفته و آمریکا به‌عنوان هستهٔ مرکزی در این شبکه ایفای نقش می‌کند.

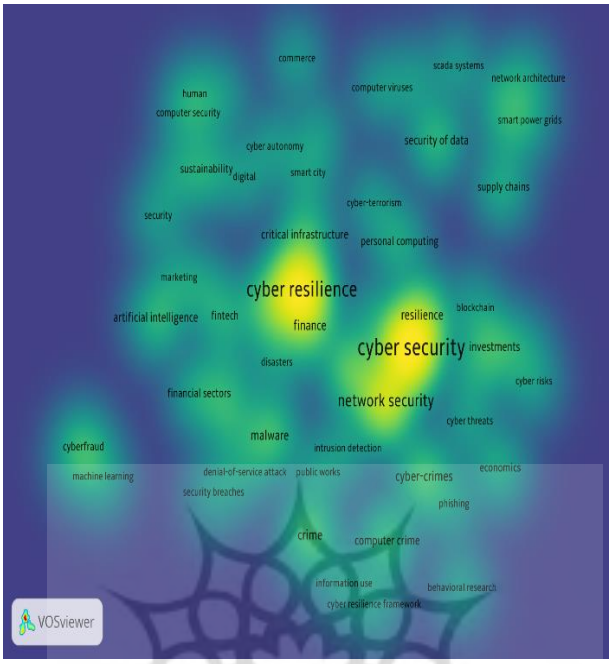


شکل ۱۰. شبکه همکاری کشورها

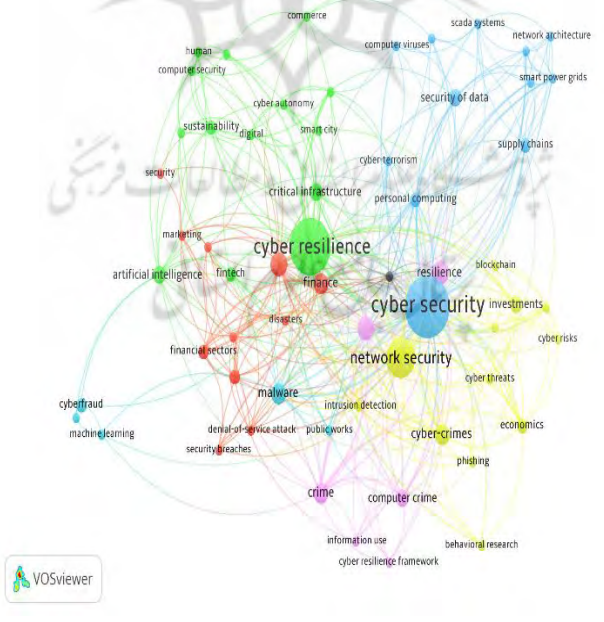
در پاسخ به سؤال چهارم به تحلیل شکل‌های زیر پرداخته می شود: تحلیل نقشهٔ هم‌واژگانی شکل‌های ۱۱ و ۱۲ نشان می‌دهد که ادبیات علمی تاب‌آوری سایبری در قالب هفت خوشهٔ اصلی سازمان یافته است. خوشهٔ آبی روشن با محوریت امنیت سایبری[1] و امنیت شبکه[2] بیشترین تمرکز را بر ابعاد فنی همچون حملات سایبری، جرایم رایانه‌ای و امنیت داده‌ها دارد. خوشه سبز بر تاب‌آوری سایبری و پیوند آن با مدیریت ریسک[3]، سرمایه‌گذاری، بخش‌های مالی، و اکوسیستم‌ها متمرکز است و پیوند مستقیمی با مدیریت ریسک و استمرار کسب‌وکار نشان می‌دهد. خوشهٔ قرمز حوزهٔ مالی و فناوری‌های نوین مانند هوش مصنوعی، فین‌تک، و کلاهبرداری سایبری را برجسته می‌سازد که بیانگر اهمیت نوآوری فناورانه و تهدیدات مالی است. خوشهٔ مشکی کوچکترین اما مستقل‌ترین خوشه است که تنها شامل ارزیابی ریسک بوده و نقش آن به‌عنوان رویکردی کلیدی برای ارزیابی و طراحی استراتژی‌های تاب‌آوری در حال تقویت است. خوشهٔ بنفش ابعاد سیاست‌گذاری، مقررات، و تاب‌آوری اجتماعی–سازمانی را پوشش می‌دهد و بر مفاهیمی چون تاب‌آوری[4]، مقررات[5]، و امنیت داده‌ها تأکید دارد. خوشهٔ فیروزه‌ای بر زیرساخت‌های حیاتی[6]، شهر هوشمند[7] و خودمختاری سایبری[8] متمرکز است که تلاقی تاب‌آوری سایبری با پایداری و تحول دیجیتال را برجسته می‌سازد. در نهایت، خوشهٔ زرد به‌عنوان خوشه‌ای نوظهور مطرح

1. Cyber security
2. Network security
3. Risk management
4. Resilience
5. Regulation
6. Critical infrastructure
7. Smart city
8. Cyber autonomy

اســت که موضــوعاتی همچون پایداری، تجارت، امنیت، و تشــخیص نفوذ[1]را در پیوند با تاب‌آوری ســایبری دنبال می‌کند. این سازمان‌یافتگی خوشه‌ای بیانگر آن است که پژوهش‌ها در این حوزه رویکردی چندبُعدی شامل ابعاد فنی، اقتصادی-مالی، اجتماعی-مقرراتی، و زیرساختی را دنبال کرده و زمینه‌ساز توسعهٔ چارچوب‌های جامع تاب‌آوری سایبری هستند.



شکل ۱۱. نقشه تراکم هم‌واژگانی



شکل۱۲. شبکه هم‌واژگانی

و در جدول ۴ به‌طور خلاصه نتایج خوشه های هم‌واژگانی آورده شده است.

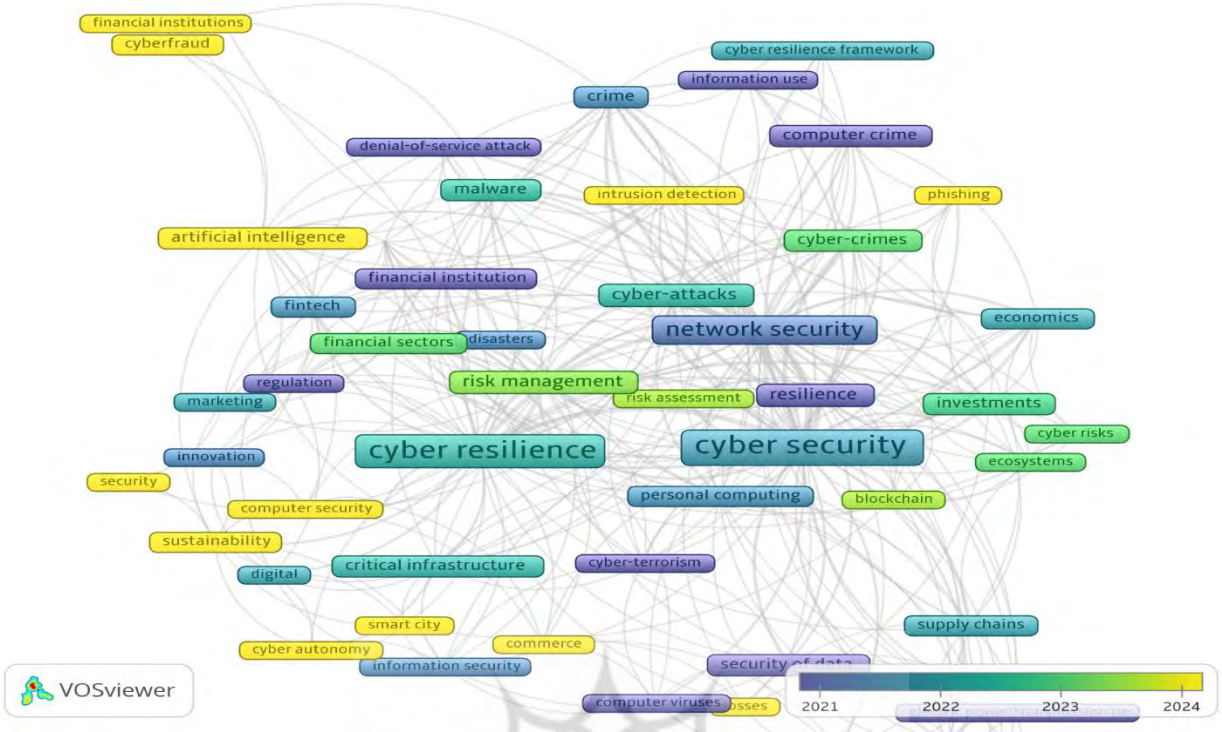
1. intrusion detection

جدول ۴. نتایج هم‌واژگانی شکل های ۱۱ و ۱۲

رنگ خوشه	کلیدواژه‌های اصلی	جهت‌گیری پژوهشی / تمرکز اصلی
آبی روشن	Cyber security, Network security, Cybercrime, Malware, DOS attack	ابعاد فنی و تهدیدات کلاسیک سایبری؛ تمرکز بر حملات، آسیب‌پذیری‌ها، و ابزارهای دفاعی
سبز	Cyber resilience, Risk management, Finance, Investment, Ecosystem	تاب‌آوری سایبری در حوزه‌های مالی و سازمانی؛ پیوند مدیریت ریسک با تداوم خدمات و اقتصاد دیجیتال
قرمز	Artificial intelligence, Fintech, Cyberfraud, Marketing, Financial institutions	ورود فناوری‌های نوین به حوزهٔمالی؛ استفاده از هوش مصنوعی برای مقابله با تهدیدات و کلاهبرداری سایبری
مشکی	Risk assessment	کوچکترین خوشه؛ تمرکز مستقل بر ارزیابی ریسک به‌عنوان رویکردی کلیدی در طراحی استراتژی‌های تاب‌آوری
بنفش	Regulation, Resilience, Data protection, Behavioral aspects	جنبه‌های سیاستی-قانونی و اجتماعی؛ نقش مقررات، حاکمیت داده، و رفتار سازمانی در تقویت تاب‌آوری
فیروزه‌ای	Critical infrastructure, Smart city, Cyber autonomy, public infrastructure	پیوند تاب‌آوری با پایداری و زیرساخت‌های حیاتی؛ تمرکز بر شهر هوشمند و خودمختاری سایبری
زرد	Sustainability, Blockchain, Supply chain, Commerce, Innovation, Data security, Intrusion detection	خوشهٔ نوظهور؛ ترکیب تاب‌آوری با فناوری‌های تحول‌آفرین (بلاک‌چین، نوآوری، زنجیره تأمین) و ابعاد توسعهٔ پایدار

روندهای نوظهور: بررسی روندهای زمانی نشان می‌دهد که در سال‌های اخیر، ادبیات تاب‌آوری سایبری به سمت مفاهیم نوظهور و بین‌رشته‌ای حرکت کرده است. واژگانی چون بلاک‌چین، زنجیره تأمین، پایداری ، شهر هوشمند، اقتصاد دیجیتال و تجارت[1] ، نوآوری، امنیت داده‌ها، امنیت رایانه، خودمختاری سایبری[2]، نهادهای مالی، کلاهبرداری سایبری[3] ، و هوش مصنوعی بیانگر گسترش رویکردها از تهدیدات فنی سنّتی به‌سوی موضوعات اجتماعی، اقتصادی، و فناورانه‌اند. این روندها نشان می‌دهند که تاب‌آوری سایبری دیگر تنها به‌عنوان یک مبحث امنیتی مطرح نیست، بلکه به ابعاد گسترده‌تری چون مدیریت زنجیره تأمین، تحول دیجیتال، اعتماد در نظام‌های مالی، توسعهٔ پایدار، و نوآوری فناورانه گره خورده است. به این ترتیب، رویکرد آیندهٔ پژوهش در این حوزه بیشتر معطوف به ادغام فناوری‌های تحوّل‌آفرین (مانند بلاک‌چین و هوش مصنوعی) با ملاحظات اقتصادی و اجتماعی برای تقویت پایداری و انعطاف‌پذیری سیستم‌های سایبری خواهد بود.

1. commerce
2. cyber autonomy
3. cyberfraud



شکل ۱۳. روندهای موضوعات نوظهور

در پاسخ به سؤال پنجم این مطالعه، تحلیل علم‌سنجی نشان می‌دهد که در حوزهٔ تاب‌آوری سایبری نظام‌های مالی و بانکی چند شکاف اصلی وجود دارد: تمرکز غالب پژوهش‌ها بر تهدیدات فنی سنتی مانند بدافزار و حملات شبکه‌ای، در حالی‌که موضوعات پیچیده‌تری همچون ریسک‌های سیستمی، اختلال زنجیره تأمین مالی، و تاب‌آوری نهادی کمتر بررسی شده‌اند؛ پراکندگی و کمبود مطالعات تجربی در زمینهٔ فناوری‌های نوظهور مانند هوش مصنوعی، بلاکچین و فین‌تک[1]؛ و محدودیت همکاری‌های میان‌رشته‌ای و بین‌المللی که مانع شکل‌گیری درک جامع و جهانی از این حوزه می‌شود. همچنین، خوشهٔ مستقل ارزیابی ریسک هنوز توسعهٔ کافی نیافته و نیازمند چارچوب‌های تلفیقی برای پیوند با راهبردهای کلان تاب‌آوری است. نتایج علم‌سنجی می‌تواند جهت‌گیری پژوهش‌های آینده را با تمرکز بر چندبُعدی سازی رویکردها (فنی، مالی-اقتصادی، اجتماعی-مقرراتی، و زیرساختی) و کاربردی سازی فناوری‌های نوظهور هدایت کند. از منظر سیاست‌گذاری نیز یافته‌ها نشان می‌دهند که چارچوب‌های نظارتی باید فراتر از امنیت سایبری سنتی رفته و بر تاب‌آوری سیستمی تأکید نمایند؛ به‌گونه‌ای که نهادهای مالی توان تحمل و بازیابی در برابر شوک‌های فناورانه و اقتصادی را داشته باشند. بدین‌ترتیب، علم‌سنجی به‌مثابه نقشهٔ راه راهبردی می‌تواند هم مسیر پژوهش‌های آینده و هم سیاست‌گذاری‌های مؤثر در تقویت تاب‌آوری سایبری نظام‌های مالی و بانکی را مشخص سازد.

۵. نتیجه‌گیری

یافته‌های این پژوهش نشان داد که تاب‌آوری سایبری در نظام‌های مالی و بانکی طی سال‌های اخیر به یک حوزهٔ پُررشد و چندبُعدی تبدیل شده است که مسیر تکاملی آن از مطالعات فنی و مفهومی اولیه به‌سمت چارچوب‌های عملی، میان‌رشته‌ای، و کاربردی‌تر حرکت کرده است. تحلیل روندها بیانگر آن است که ادبیات این حوزه پس از یک دوره شکل‌گیری اولیه، در سال‌های اخیر با جهشی

1. FinTech

چشمگیر مواجه شده و اکنون در نقطه‌ای قرار دارد که نه‌تنها به تهدیدات سنتی، بلکه به ابعاد پیچیده‌تری همچون ریسک‌های سیستمی، تاب‌آوری زنجیره تأمین مالی، اعتماد مشتری، و حکمرانی سایبری می‌پردازد. بررسی خوشه‌های موضوعی نشان داد که پژوهش‌ها در هفت محور کلیدی سازمان یافته‌اند؛ از امنیت فنی و مدیریت ریسک گرفته تا زیرساخت‌های حیاتی، مقررات، نوآوری‌های فناورانه، و ابعاد پایداری اقتصادی-اجتماعی. روندهای نوظهور مانند بلاک‌چین، هوش مصنوعی، فین‌تک، شهر هوشمند، و پایداری نیز گویای تغییر جهت ادبیات به‌سمت پیوند تاب‌آوری سایبری با فناوری‌های تحوّل‌آفرین و توسعهٔ پایدار هستند. در سطح همکاری‌های علمی، الگوها نشان دادند که شبکه‌های پژوهشی هنوز محدود و متمرکز بر چند کشور و مؤسسهٔ پیشرو هستند، درحالی‌که تقویت همکاری‌های میان‌رشته‌ای و فراملی می‌تواند درک جامع‌تری از پویایی‌های این حوزه فراهم سازد. علاوه‌براین، خوشهٔ مستقل ارزیابی ریسک بیانگر خلأ مهمی است که باید در پژوهش‌های آتی با توسعهٔ چارچوب‌های یکپارچه برای سنجش و مدیریت ریسک در نظام‌های مالی پُر شود. از منظر سیاست‌گذاری، نتایج این پژوهش آشکار می‌سازد که چارچوب‌های نظارتی آینده باید فراتر از رویکردهای سنتی «پیشگیری و حفاظت» رفته و بر تاب‌آوری سیستمی متمرکز شوند؛ به‌گونه‌ای که نهادهای مالی توانایی مقاومت، بازیابی، و سازگاری در برابر شوک‌های فناورانه و اقتصادی را داشته باشند. این امر مستلزم سرمایه‌گذاری در همکاری‌های میان‌رشته‌ای، توسعهٔ ظرفیت نهادی، و کاربردی‌سازی فناوری‌های نوظهور است. بدین‌ترتیب، تحلیل علم‌سنجی نه‌تنها وضعیت موجود را ترسیم می‌کند، بلکه به‌عنوان یک نقشهٔ راه راهبردی می‌تواند مسیر پژوهش‌های آینده و تدوین سیاست‌های مؤثر برای ارتقاء تاب‌آوری سایبری در نظام‌های مالی و بانکی را هدایت کند.

این پژوهش با وجود جامعیت نسبی، محدودیت‌های دارد. نخست، داده‌ها صرفاً از پایگاه اسکوپوس استخراج شده‌اند و بنابراین ممکن است بخشی از مقالات نمایه‌شده در سایر پایگاه‌ها (مانند وب‌آوساینس یا گوگل اسکالر) در تحلیل وارد نشده باشند. دوم، تحلیل‌ها به مقالات انگلیسی محدود بوده و ادبیات غیرانگلیسی (به‌ویژه در کشورهای در حال توسعه) نادیده گرفته شده است. سوم، روش علم‌سنجی گرچه برای ترسیم تصویر کلان بسیار کارآمد است، اما قادر به ارائهٔ تحلیل‌های عمیق محتوایی و کیفی از مقالات نیست.

پیشنهادهایی برای آینده

بر مبنای یافته‌ها و محدودیت‌ها، مسیرهای متعددی برای پژوهش‌های آینده قابل ترسیم است:

۱. گسترش دامنه تحلیل با بهره‌گیری از چند پایگاه داده و پوشش مقالات به زبان‌های مختلف.
۲. تلفیق روش‌های علم‌سنجی کمّی با تحلیل‌های کیفی و محتوایی برای درک عمیق‌تر از الگوهای پژوهشی.
۳. تمرکز بیشتر بر مطالعات تجربی و موردی در حوزهٔ بانک‌ها و مؤسسات مالی واقعی به‌جای مدل‌های صرفاً مفهومی.
۴. توسعهٔ چارچوب‌های ارزیابی ریسک یکپارچه که ابعاد فنی، نهادی، و اقتصادی را توأمان در نظر بگیرد.
۵. بررسی تأثیر همکاری‌های میان‌رشته‌ای و بین‌المللی بر ارتقاء تاب‌آوری سایبری در سطح سیستم‌های مالی جهانی.

فهرست منابع

Adriaanse, L., & Rensleigh, C. (2013). Web of Science, Scopus and Google Scholar: A content comprehensiveness comparison. The Electronic Library, 31(6), 727–744. https://doi.org/10.1108/EL-12-2011-0174

Alharbi, F. (2025). Twelve years of cyber resilience: Analyzing cyberattacks in Saudi Arabia (2012–2024). *TEM Journal*, *14*(2), 1791–1807. https://doi.org/10.18421/TEM142-77

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. Computers & Industrial Engineering, 149, 106829. https://doi.org/10.1016/j.cie.2020.106829

Bakhmat, N., Kolosova, O., Demchenko, O., Ivashchenko, I., & Strelchuk, V. (2022). Application of international scientometric databases in the process of training competitive research and teaching staff: Opportunities of Web of Science (WoS), Scopus, Google Scholar. In Proceedings [Conference paper]. https://www.jatit.org/volumes/Vol100No13/21Vol100No13.pdf?utm_source

Belhadi, A., Mani, V., Kamble, S., Khan, S. A. R., & Verma, S. (2021). Artificial intelligence-driven innovation for enhancing supply chain resilience and performance under the effect of supply chain dynamism: An empirical investigation. N/A. https://doi.org/10.1007/s10479-021-03956-x

Benoît Dupont. (2019). The cyber-resilience of financial institutions: Significance and applicability. Journal of Cybersecurity, 5(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

Board of Governors of the Federal Reserve System. (2024). Financial Stability Report - April 2024. Federal Reserve. Retrieved from https://www.federalreserve.gov/publications/April-2024-financial-stability-report-purpose-and-framework.htm

Burnham, J. F. (2006). Scopus database: A review. Biomedical Digital Libraries, 3(1), 1. https://doi.org/10.1186/1742-5581-3-1

Cojocaru, A. (2025). Aligning regulation and governance for cyber resilience: A theoretical framework for the UK financial sector. Computers & Security, 157, 104627. https://doi.org/10.1016/j.cose.2025.104627

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research, 133, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. Journal of Cybersecurity, 5(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

Eghtesad Online. (2025, June 17). Cyberattack on Iran's banking network [in Persian]. https://www.eghtesadonline.com/fa/news/2067531

Federal Reserve. (2022). Implications of cyber risk for financial stability. FEDS Notes. https://ideas.repec.org/p/fip/fedgfn/2022-05-12.html?utm_source

FSB (Financial Stability Board). (2020). Effective practices for cyber incident response and recovery . https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery/?utm_source

Godbole, T., Gochhait, S., & Ghosh, D. (2022). Developing a framework to measure cyber resilience behaviour of Indian bank employees. In T. Senjyu, P. N. Mahalle, T. Perumal, & A. Joshi (Eds.), ICT with intelligent applications. Smart Innovation, Systems and Technologies, 248. Springer, Singapore. https://doi.org/10.1007/978-981-16-4177-0_31

Groenendaal, J., & Helsloot, I. (2021). Cyber resilience during the COVID-19 pandemic crisis: A case study. Risk Analysis, 41(6), 1116–1130. https://doi.org/10.1111/1468-5973.12360

Gündüzyeli, B. (2025). Cyber resilience in digital marketing within the framework of sustainable management. Sustainability, 17(5), 2080. https://doi.org/10.3390/su17052080

Hagan, M., Tummala, R., & Williams, S. (2019). Enhancing security and privacy of next-generation edge computing technologies. In Proceedings of the International Conference on Privacy, Security and Trust (PST). IEEE. https://doi.org/10.1109/PST47121.2019.8949052

Herburger, M., Wieland, A., & Moller, D. (2024). Building supply chain resilience to cyber risks: A dynamic capabilities perspective. Supply Chain Management. https://doi.org/10.1108/SCM-01-2023-0016

Hua, J., Bapna, S., & Ray, S. (2018). Are we ready for cyberterrorist attacks?—Examining the role of individual resilience. Information & Management, 55(7), 997–1007. https://doi.org/10.1016/j.im.2018.04.008

Köhler, J., Geels, F. W., Kern, F., Markard, J., Onsongo, E., Wieczorek, A., Alkemade, F., Avelino, F., Bergek, A., Boons, F., Fünfschilling, L., Hess, D., Holtz, G., Hyysalo, S., Jenkins, K., Kivimaa, P., Martiskainen, M., McMeekin, A., Mühlemeier, M. S., Nykvist, B., Pel, B., Raven, R., Rohracher, H., Sandén, B. A., Schot, J., Sovacool, B. K., Turnheim, B., Welch, D., & Wells, P. (2019). An agenda for sustainability transitions research: State of the art and future directions. N/A. https://doi.org/10.1016/j.eist.2019.01.004

Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M.-V. (2018). Resilience and cybersecurity: Emerging challenges in the digital age. Springer.

López-Pernas, S., Saqr, M., & Apiola, M. (2023). Scientometrics: A concise introduction and a detailed methodology for mapping the scientific field of computing education research. In *Past, Present and Future of Computing Education Research: A Global Perspective*. https://www.scopus.com/pages/publications/85197199852

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2019). A culture of cybersecurity at Banca Popolare di Sondrio. In Proceedings of AMCIS 2019. AIS Electronic Library. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/24

Martín-Martín, A., Orduna-Maléa, E., Thelwall, M., & Delgado López-Cózar, E. (2018). Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories. arXiv:1808.05053. https://doi.org/10.1016/j.joi.2018.09.002

Martín-Martín, A., Orduna-Maléa, E., Thelwall, M., & Delgado López-Cózar, E. (2020). Google Scholar, Microsoft Academic, Scopus, Dimensions, Web of Science, and OpenCitations' COCI: A multidisciplinary comparison of coverage via citations. Scientometrics, 124(3), 2683–2710. https://doi.org/10.1007/s11192-020-03690-4

Maurer, T., & Nelson, A. (2021). The global cyber threat to financial systems. Finance & Development, 58(1). https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

Ogasawara, N. (2024). A global view of hepatology collaboration: Insights and future directions from 30 years of network analysis (1994–2023). *Arquivos de Gastroenterologia*. https://www.scopus.com/pages/publications/85213469300

Ogasawara, N. (2025). Three decades of collaboration in rheumatology: A comprehensive co-authorship network analysis (1994–2023). Reumatologia https://www.scopus.com/pages/publications/105004191633

Puente, J. H., Lucero-Baldevenites, E. V., Díaz-Chieng, L. Y., & Roman-Acosta, D. (2024). Tools and methodologies for scientific evaluation: Bibliometrics, scientometrics and informatics. Seminars in Medical Writing and Education. https://www.scopus.com/pages/publications/105000249716

Saha, B., & Saha, U. (2024). Cyber resilience calculator: A game-changer for small to mid-sized businesses in allocating information technology security budgets effectively. In 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (pp. 1–6). IEEE. https://doi.org/10.1109/ETNCC63262.2024.10767460

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2024). The state of cyber resilience: Advancements and future directions. In A. K. Nagar, D. S. Jat, D. K. Mishra, & A. Joshi (Eds.), Intelligent sustainable systems. WorldS4 2023. Lecture Notes in Networks and Systems, 817. Springer, Singapore. https://doi.org/10.1007/978-981-99-7886-1_30

Seid, E., Blix, F., & Popov, O. (2025). Cyber resilience using ASFA: DORA-compliant threat-led penetration testing. In G. Oliva, S. Panzieri, B. Hämmerli, F. Pascucci, & L. Faramondi (Eds.), Critical information infrastructures security. CRITIS 2024. Lecture Notes in Computer Science, 15549. Springer, Cham. https://doi.org/10.1007/978-3-031-84260-3_16

Shekofteh, M., Mohseny, M., Shahbodaghi, A., & Rahimi, F. (2016). The correlation among Y-index and other scientometric indicators. Current Science. Retrieved from https://www.scopus.com/pages/publications/84969577699

Prabhu, S. G., Ashok, P., & Ramesh, K. (2024). Cyber resilience: Safeguarding India's markets in the post-pandemic cyber landscape. In 2024 International Conference on IT and Platform Management (ICIPTM). IEEE. https://doi.org/10.1109/ICIPTM59628.2024.10563229

Vernotte, A., Apvrille, L., & Roudier, Y. (2018). Load balancing of renewable energy: A cyber security analysis. Energy Informatics, 1(1), 10. https://doi.org/10.1186/s42162-018-0010-x

Vishwanath, A., Neo, L. S., Phua, J., & Ong, G. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 130, 113160. https://doi.org/10.1016/j.dss.2019.113160

Yao, L.-Y., Chen, K.-Y., & Lyu, P.-H. (2025). Academic collaboration networks study on library and information science community. Scientometrics .www.scopus.com/pages/publications/105011408166